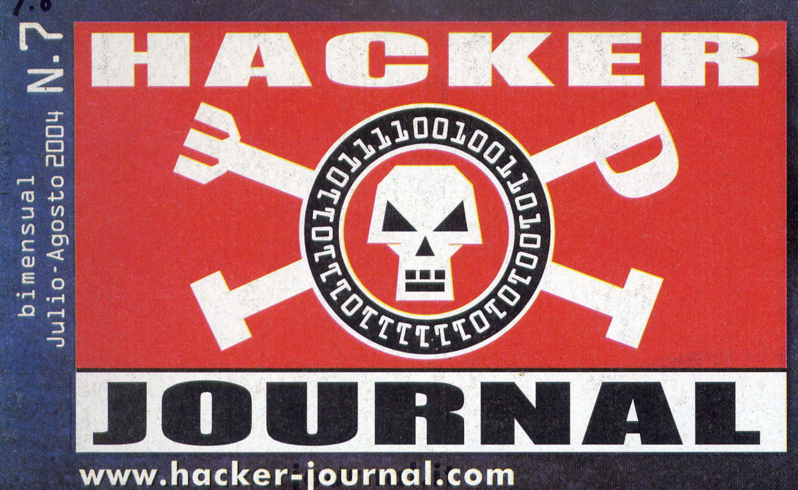
bimensual
Julio-Agosto 2004
N.7

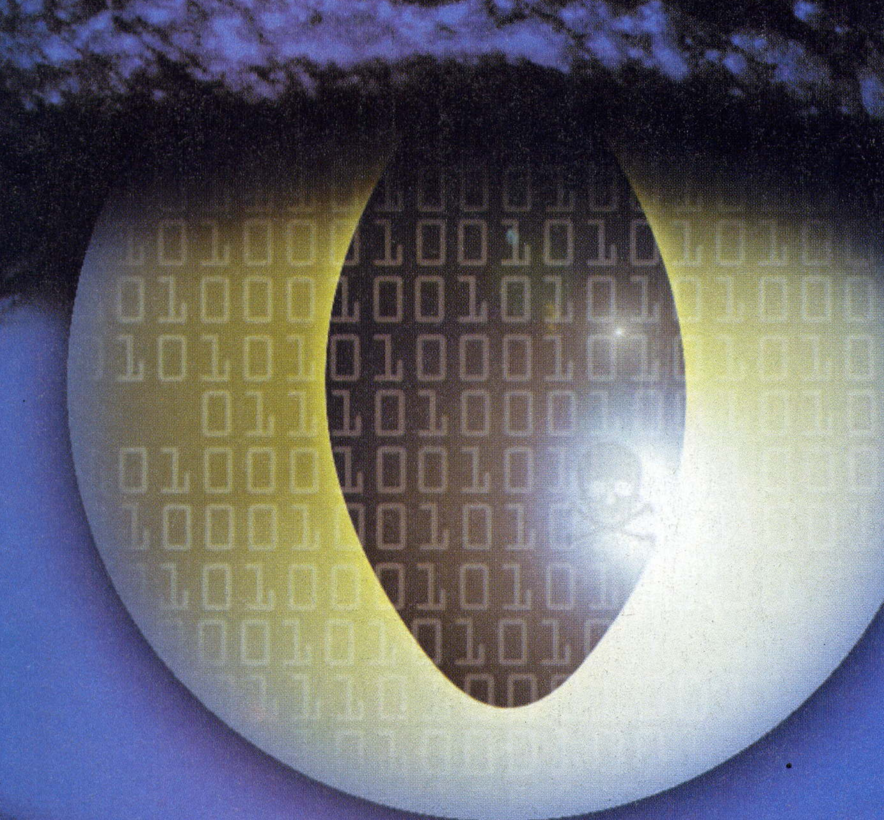


www.hacker-journal.com

ENGAÑAR AL SPYWARE

SI LO CONOCES, LO EVITAS

2€
SIN PUBLICIDAD
SÓLO INFORMACIÓN Y ARTÍCULOS



OCULTANDO

un archivo dentro de otro

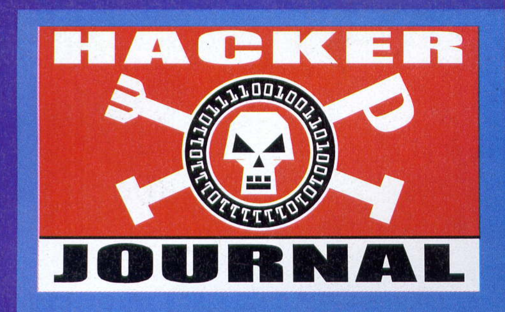
SERVIDORES PINCHADOS
¡Descúbrelos en seguida!

Ingeniería social
Una llamada de 10 millones de dólares

Piratas chinos: ¿románticos?

00007

4€



Año 2 - N. 7
Julio-Agosto 2004

Director Responsable:
Luca Sprea

Los chicos de la redacción europea:
Federico Cociancich, Amadeu Brugués, Infoambiente, Gualtiero Tronconi, Eduardo Bracaglia, Gregorio Peron, Contents by MDR

Colaboradores: Bismark, Fabio Benedetti, Guillermo Cancelli, Gaia, Nicolás A., Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia,3dO, Mònica Batalla, Anna Riera

Maquetación: Estudi Digital, S.L.

Diffusión: Paul-Luc Perez

Redacción
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printed in Italy

Distribución
Coedis, S.L. - Avda. de Barcelona 225
08750 Molins de Rei (Barcelona)

Publicación bimensual registrada el 14/2/03 con el número MI2003C/001404

hack·er (hăk'ər)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios que prefieren aprender solamente lo mínimo necesario."

SABER Y RECORDAR

Durante el mes de junio se celebra en Europa y Norteamérica el desembarco de Normandía, cuando, hace ahora sesenta años, miles de soldados en su mayor parte estadounidenses, canadienses y británicos realizaban un desembarco masivo que sería el principio del fin de la II Guerra Mundial.

Sin embargo, no todos recuerdan que, mientras se libraban duras batallas en el continente, se desarrollaba una menos cruenta pero no menos importante guerra entre servicios de inteligencia. Los aliados echaron el resto para comprender y descifrar la máquina Enigma, responsable del cifrado de las comunicaciones del bando alemán.

Y en esta guerra de espías, en la que los contendientes batallaban principalmente con su inteligencia, brilla con luz propia la aportación de Alan Turing, el hombre clave para descifrar el código y que, de paso, sentó muchas de las bases de la informática tal y como hoy la conocemos. Sigue siendo célebre el test de Turing para analizar la inteligencia artificial, según el cual, cuando en un diálogo sin contacto sensorial directo con los interlocutores, uno no sea capaz de discriminar si dialoga con un humano o con una máquina, se habrá conseguido la inteligencia artificial verdadera. Mientras esperamos la llegada de este logro teórico, los matemáticos tienen trabajo de sobra con la máquina de Turing, modelo teórico que Alan Turing formuló en 1936 y que trabaja con una cinta infinita de ceros y unos. A partir de los principios de esta "sencilla" máquina, los ordenadores siguen progresando sin moverse ni un ápice de sus postulados fundamentales, y los mejores matemáticos empiezan a tener problemas para discriminar dónde acaba la matemática pura y dónde empieza la filosofía. Con preguntas de tal calado, a nosotros nos queda al menos la cuestión ética de base: ¿qué uso hacemos de la tecnología para relacionarnos con nuestros semejantes? No es una pregunta banal: jamás los simples mortales hemos estado tan cerca de dejar el mundo mejor que cuando llegamos.

redaccion@hacker-journal.com

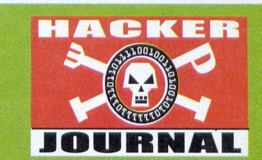
UNA REVISTA PARA TODOS


NEWBIE


MID HACKING


HARD HACKING

El mundo hacker se compone de algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal está marcado con una clave para cada nivel: NEWBIE (para quien comienza), MIDHACKING (para quien ya está dentro) y HARDHACKING (para quien no existen los secretos).



Número 7 - Julio - Agosto 2004

02 - Editorial
04 - Correo
06 - Noticias
08 - Engañar al Spyware. Programas espía: si los conoces, los evitas. O sabes cómo liberarte.
10 - ¡Descubre los servidores pinchados!
12 - Una llamada de 10 millones de dólares
14 - Piratas chinos: Nacionalistas, instrumentalizados pero románticos
16 - Como un cubo de la basura
18 - Microsoft es tirar el dinero
20 - Código nazi: simple y eficaz
22 - Escuchar a la policía
23 - Ocultando un archivo: cómo ocultar un mensaje dentro de otro
26 - Custom Right Click!
28 - Windows: el password no sirve de nada
30 - Regla número uno: Haz que te encuentren

SITIO WEB

¡La Secret Zone ya está en marcha! De acuerdo, hemos tardado. Pero por fin está activada y en ella podéis encontrar ya los primeros números de Hacker Journal. Si os habéis perdido algún número anterior, ya sabéis dónde están.

¿Os gusta la Secret Zone? Escribidnos a redaccion@hacker-journal.com

Visita nuestro sitio web: **www.hacker-journal.com**



¡SECRET ZONE RELOADED!

Por un problema técnico, hasta ahora la Secret Zone estaba fuera de combate. Pero eso se acabó: ya podéis entrar en ella desde el sitio web, donde encontraréis los números 1 y 2 de Hacker Journal en formato PDF. Poco a poco iremos incorporando más números anteriores, para que no os perdáis ninguno. Con algunos navegadores, puede ser necesario insertar dos veces los mismos códigos. No os detengáis al primer intento

user: secre7
password: p0rf1n

Try2Hack

TRY2HACK

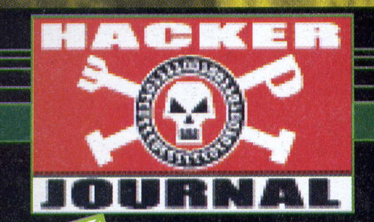
[NEWS] - [FAQ] - [RULES] - [CHAT] - [CREDITS]

LEVEL 1

Enter the password below to continue:

click here to continue

También está operativo el link a Try2Hack. Se trata de un sitio donde puedes probar a hackear páginas una tras otra y comprobar tu nivel de conocimientos. Si te pierdes, busca por los foros...



mailto:
redaccion@hacker-journal.com

NUEVO WEB

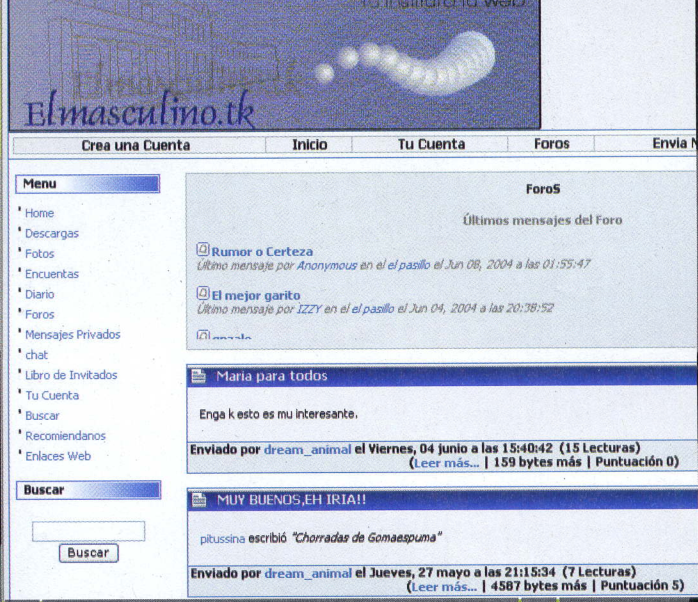
Salu2!

En primer lugar felicitaros x la reviste ke es 1 pasada...Somos 1 grupo de estudiantes de BAC en Lugo y hemos hecho 1 web del instituto kon exámenes, apuntes....ke poko a poko iremos metiendo (aun estamos en construcción). ¿Seríais tan amables de poner nuestra web en vuestra revista? Es http://elmasculino.tk. Muchísimas gracias.
En nombre de los admin :Hunk, dream_animal y monchiny

Stamos deseando ke el proximo numero salga al kiosko!

Hunk

¡Pues aquí dejamos el testimonio escrito de vuestro sitio web, para que lo visite quien quiera ver vuestro encomiable trabajo!



ESCRIBIR ARTÍCULOS

Saludos.
Desde hace tiempo me ha gustado vuestra revista, así que me he decidido a ponerme en contacto con vosotros para saber si existe la posibilidad de escribir artículos para Hacker Journal, o de lo contrario, el grupo es cerrado.
Estoy bastante interesado en participar con HJ.
Me mantengo a la espera de respuesta, gracias por anticipado.

Tresde

Por supuesto que sí. Como seguro sabes bien, la revista cuenta con un web, www.hacker-journal.com, donde tienen cabida las colaboraciones de nuestros lectores. Si quieres colaborar, puedes entrar en el sitio y mandarnos desde allí tus trabajos, donde estarán al alcance de todos los visitantes. ¡Anímate a escribir!

TRABAJO DE CHINOS

Estimados amigos:

Tengo una idea muy justa de ordenadores, solo a nivel de usuario, y leo vuestra revista para ir entendiendo mas el entorno de trabajo. Gracias a ella uno se va volviendo menos torpe.

Os propongo estas líneas mías que pueden hacer un pequeño recuadro anecdótico o un mini artículo que sea quizás interesante. Puedo rescribir o completar lo escrito si hace falta. Pueden disponer del texto libremente. Mi ordenador tiene instalado el Njstar comunicator que interpreta los signos en chino para completar el artículo y los ejemplos, pero es inútil mandarles signos en chino junto a las palabras en pinyin si no está en el suyo pues quedan como cuadraditos blancos. Si les parece interesante podemos buscar la forma de hacérselo llegar. El artículo es correcto hasta donde se, aunque sea una simplificación de la complejidad del idioma.

TRABAJO DE CHINOS

Mas de una vez hemos visto en alguna película como el héroe, un "ta bi ze" (narizotas) occidental, se abalanza decidido a detener el contador de la bomba nuclear, se coloca sobre el teclado, y... se queda a cuadros viendo un sin fin de garabatos sobre el teclado.

¡Diantre! ¡¡Es un teclado chino!!
Pero, ¿cómo se escribe con un teclado en chino? Para entender la respuesta, necesitamos un par de conocimientos básicos sobre su idioma, tan bello y tan diferente del nuestro.

LOS RADICALES

El idioma chino no puede descomponerse en palabras o en letras ,es un idioma constituido por radicales. Cada raíz, o radical, es un fonema y a la vez una idea o significado, un golpe de voz al que le corresponde un símbolo. Así, "nu" por ejemplo, es mujer (y se escribe *)
Sin embargo estos fonemas se combinan para dar conceptos derivados de ellos, con la complicación añadida de que al hacerlo pueden cambiar por completo el fonema original. Así siguiendo con nuestro ejemplo, "bueno" en chino es "hao", que resulta de combinar los signos "nu"(mujer) y "zi" (niño), que viene de la idea de que una mujer con un niño es algo bueno. Como vemos, el símbolo conjunto se pronuncia "hao" como resultado de combinar los dos radicales, y no "nu-zi" como podríamos pensar en un principio.
¿Suena complicado? Pues la cosa no ha hecho más que empezar. Aparte del número de combinaciones fonéticas, gráficas, y de conceptos, contamos con una complicación añadida. En chino existen cuatro tonos, que podemos llamar llano, ascendente, curvo, y descendente. El mismo fonema, pronunciado con diferente tono, tiene un signo diferente y significa algo distinto, por lo que necesitamos un oído fino y mucha práctica para apreciar el tono del monosílabo que oímos.
Muy bien, tenemos al menos doscientos signos , fonemas y no tenemos letras para combinar formando palabras, sino que combinamos sonidos y/o ideas. Tampoco tenemos doscientas teclas, una por signo o fonema, para hacer las combinaciones. Ni siquiera podemos ir pintando cada uno de los trazos que tiene el símbolo a diferente altura y posición, pues sería demasiado lento y complicado, más un trabajo de dibujo que de escritura.

HABLANDO COMO LAS PALOMAS

¿Cómo se corresponde el idioma de signos ideográficos, los fonemas pronunciados, y la transcripción en símbolos del alfabeto occidental?. Esto se resuelve con el uso del chino "pinyin", que viene de la palabra inglesa "pidgeon", paloma, cuyo golpeteo de cabeza recuerda el hablar a golpes como los indios, tipo :"yo vivir España", que es una forma de decir que el idioma está simplificado.

El pinyin es fijar con letras europeas los sonidos chinos, lo que estábamos haciendo al escribir "nu"como el sonido de mujer, o "hao" como el sonido de bueno. Es decir, que el garabato en chino suena así, "hao", en su tono correspondiente, lo que se consigue con acentos.

A estas alturas los sudores ya recorren la cara y la espalda de nuestro héroe. Parece imposible desbloquear ese código. ¿Como hacemos para escribir en europeo un sonido chino y que nos salga un símbolo ideográfico en la pantalla, cuando este puede ser combinación de otros mas sencillos?

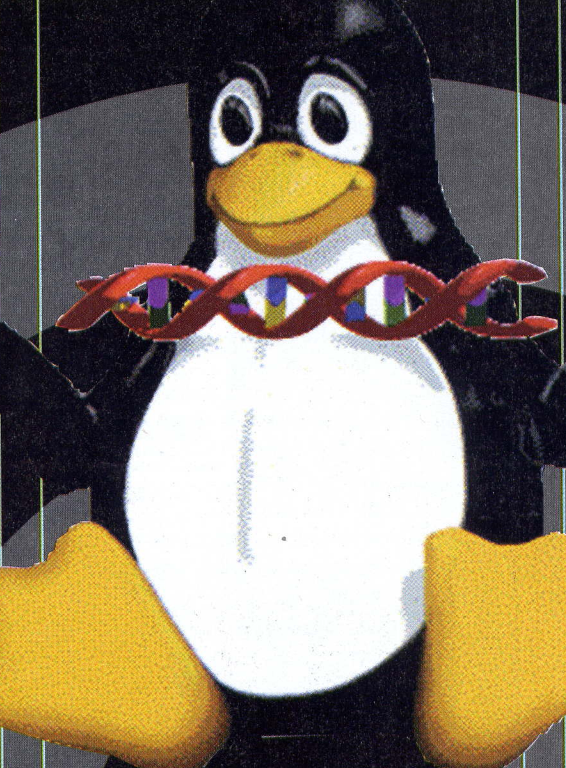
LA SOLUCIÓN: UN PROGRAMA PUENTE

El problema lo resuelve un programa puente , por ejemplo el popular NJStar Comunicator, que se puede encontrar en Internet, aunque sus opciones completas suelen ser de pago. Puede usarse para varios idiomas asiáticos, como el coreano o el japonés, aparte del chino.

Tecleamos una palabra en pinyin, como "hao" y el ordenador nos abre en una ventanita todos los signos que pueden pronunciarse así, en opción 1, 2, 3, etc, generalmente hasta media docena. Al pulsar la opción nos escribe el símbolo del garabato chino en la hoja de texto.

Con práctica se puede adquirir bastante velocidad. Además, cuando se escriben palabras compuestas se reduce el número de opciones muchas veces hasta quedar en una sola. Así "Ni Hao", o buenos días, es una única combinación posible, con lo que el programa sólo nos da una opción, y la transcribe en su forma china al texto.

Existe también otra forma abreviada, donde cada tecla corresponde a un grupo de fonemas que empiezan por el sonido del fonema. Así, la "n" pulsada sin mas, es un atajo para escribir "nu" que es el radical mas utilizado empezando por el sonido"n". Las opciones secundarias se hacen como antes, pulsando la n y a continuación la opción, lo que obliga a conocer de qué tecla y opción puede salir el radical. Un ejercicio de memoria al que se acostumbran rápidamente, pudiendo localizar rápidamente la combinación tecla-opción que les lleva directamente al radical deseado. Cuando el teclado es chino y no con letras europeas, es esto lo que vemos.



Nuestro héroe ya puede traducir el código. ¡Siempre que sepa como hablar en chino, claro! Porque usar un diccionario chino a partir de un orden fonético y por número de trazos es parte de otra lección.

Alex Martínez

¿Qué decir? Tenemos que reconocer que en alguna ocasión, husmenando por la red, hemos ido a parar a páginas web en chino, y nos sonaban a eso, a chino. Por suerte (para nosotros), muchas de estas páginas están traducidas al inglés, y nos íbamos como un rayo a ellas. Si no existe traducción, no hay visita... ¡Ahora, gracias a tu magnífica exposición, al menos ya sabemos lo que nos estamos perdiendo! Lo que podemos asegurarte es que ya no podremos volver a mirar nuestro salvapantallas de Matrix con los mismos ojos que antes.

MUCHA PALABRERIA

Queria dejar una opinion sobre vuestra revista y sobre los articulos que en ella publicais. Mucha palabrería, gigante de Redmon, Bill Bates, software libre, freedom, open source,... Mucho cartel, pero todas las herramientas y referencias a "técnicas" son sobre el mismo software, el de Microsoft. Es patético, la verdad, y el contenido deja mucho que desear...por no decir que como contenido real no hay nada. Seguro que esto no lo publicais, ¿eh?

electro

Mmmm, parece ser que sí, que lo hemos publicado. Tu opinión es tan legítima como cualquier otra. Pero no nos resistimos a aportar un par de matices. En primer lugar, es cierto que la presencia de Windows es alta, pero es que el uso de Windows entre nuestros lectores es igualmente alto. Que esto sea o no deseable es otra cuestión, ¡pero un hacker también puede decidir ser experto en Windows!
Y en segundo lugar, los contenidos están adaptados para determinado nivel de lector, algo indispensable antes de escribir una sola letra. A unos les parecerá poco y a otros, demasiado.

ACERCA DE HACKER JOURNAL

Hola,
después de acceder por medio de los códigos de la última revista Hacker Journal 6 compruebo que por fin está disponible la versión PDF de la revista pero parece que el N°1 está incompleto (sólo hasta la pág 26, le falta de la 27 a 32). ¿Es esto normal? Pues el N°2 esta completo.
Se agradecería tambien que la portada estuviera tambien en la secret zone.
Estaria bien hacer un N° de aniversario con un SUPER CD-rom, ¿no?
Gracias por hacer este tipo de prensa (ahora no sólo escrita)...

EdouardHG

Conseguir que la Secret Zone funcionara no ha sido fácil, pero por fin la tenemos activada. Ahora es hora de resolver los "flecos" que nos indicas. Tomamos nota.

HOT!!

PÁGINAS WEB EN ESPAÑOL DEFIENDEN LA ANOREXIA Y LA BULIMIA

Un rastreo en Internet ha detectado más de 50 páginas web en español, y otras muchas en inglés, que defienden la anorexia y la bulimia como estilos de vida. En estos sitios se reúnen auténticas comunidades de adolescentes que intercambian experiencias e información a través de los foros de sus páginas. Cada página cuenta con entre 700 y 800 usuarias registradas y el número de visitas a cada una de ellas puede multiplicarse por diez. De las usuarias, un 68 por ciento son adolescentes de 14 a 17 años, un 10 por ciento son menores de 14 años, y un 22 por ciento cuentan con más de 18 años.

Además, un 70 por ciento están en la fase de inicio, cuando la enfermedad todavía no se ha desarrollado, mientras que un 23 por ciento está en fase de desarrollo y un 7 por ciento en tratamiento médico. Las páginas están perfectamente estructuradas.

La herramienta preferida de las usuarias es el 'foro', donde se intercambian información sobre dietas, trucos para engañar a los padres o técnicas de autolesión.

LAS NUEVAS TI MEJORAN EL BIENESTAR SOCIAL

Cuatro de cada cinco españoles consideran que las nuevas tecnologías de la información han contribuido a mejorar el bienestar social y casi un tercio asocia este concepto al ordenador, según los resultados del 'Estudio sobre la Actitud y Comportamiento hacia las nuevas tecnologías', realizado por TNS-Demoscopia por encargo de Intel Iberia.

Del mismo informe también se desprende que el 80% considera que la NN.TT. son el motor de la sociedad, el 92% está de acuerdo en que las NN.TT. "facilitan el trabajo", mientras que el 96% mantiene que "han cambiado las formas de trabajar".

El estudio revela que los españoles tienen una alta valoración de las nuevas tencnologías y que éstas se ven como instrumentos o dispositivos útiles que ayudan al progreso de la sociedad en diferentes áreas. Se trata, pues, de usuarios felices.

OPENWAVE SE ENFRENTA AL E-ABUSO



Openwave Systems, proveedor de productos y servicios de software abierto, ha abierto su primera conferencia europea Anti-abuso, en la que ha reunido a expertos y líderes del sector con el objetivo de combatir el mal empleo de la mensajería móvil y el correo electrónico.

Entre los ponentes del evento, concebido como un foro para debatir políticas/legislación, códigos de conducta y arquitecturas tecnológicas para una lucha efectiva contra los abusos, se han incluido a representantes de la Comisión Europea, del proyecto Spamhaus, Vodafone, Brightmail e IDC.

Así, IDC ha señalado que "hemos detectado un alto nivel de spam en el mundo SMS, que podría llegar a otros entornos de mensajería como el MMS y el correo móvil. Por este motivo, es necesario adoptar medidas que minimicen el correo electrónico no deseado y que protejan al usuario final".

Rich Wong, responsable de Openwave, indica que "los clientes finales están comprobando el efecto real que el abuso de la mensajería está teniendo en sus vidas diarias y los operadores están sintiendo el golpe que supone que los consumidores elijan a operadoras con sistemas para mantener a los productores de spam controlados. Creemos que éste y otros eventos ayudarán a la industria a centrar sus esfuerzos en la lucha contra este fenómeno".

La conferencia europea Anti-abuso de Openwave pone en común las mejores prácticas para combatir las epidemias de virus y spam en dispositivos fijos y móviles. El encuentro cuenta con el apoyo de agentes influyentes, con aportaciones propias de Phillipe Gérard, de la Dirección General de la Sociedad de la Información de la Comisión Europea y Steve Linford, director del proyecto Spamhaus.

"La avalancha de correo no deseado para usuarios móviles está a punto de producirse. Cuanto antes se reúna la industria para crear planes coordinados y arquitecturas tecnológicas que impidan que esto suceda, mejor", comenta Steve Linford, director de Spamhaus.

EL ADSL SE ESTANCA EN ESPAÑA

El número de líneas ADSL de acceso a Internet a alta velocidad aumentó en un 18,9 por ciento en los primeros cincos meses del año, 11,4 puntos menos que en el mismo periodo de 2003, según se desprende de los datos facilitados mensualmente por las operadoras a la Asociación de Internautas (AI).

Así, de enero a mayo de este año el parque español de ADSL aumentó en 313.672 líneas, hasta rozar los dos millones (1.974.119), mientras que un año antes, durante el mismo periodo, se había incrementado en 289.899 conexiones.

Respecto a las variaciones mensuales, en mayo --por segundo mes consecutivo-- volvió a disminuir el ritmo de crecimiento, al aumentar un 3,3 por ciento (63.669 líneas), sólo superior al experimentado en febrero (3,1 por ciento), pero inferior a las subidas de los meses de enero (3,8), marzo (cuatro) y abril (3,4).



NUEVOS DVD-RAM DE EMTEC

EMTEC

QUICKSEARCH GO

CONSUMO
PROFESIONAL
INDUSTRIA
CONOZCANOS
SERVICIOS
GRUPO EMTEC
CONSUMO
▸Audio
▸Video
▸Multimedia
▸Prod. Impresión
▸Promociones
▸Novedades

CONSUMO

SONIDO! Audio Consumo
Con nuestros productos, EMTEC proporciona la mayor satisfacción y placer a la hora de escuchar música. El inmenso rango de productos analógicos y digitales cumple y sobrepasa todas las especificaciones internacionales para fabricantes de equipos. Nuestros desarrollos, al son de los deseos del consumidor.

IMAGEN! Video Consumo
La rápida evolución de la tecnología en el sector de la TV y Vídeo junto con la aparición de nuevo hardware con mayores capacidades, presenta un reto para la calidad y versatilidad de medios de grabación. EMTEC aceptó este reto desarrollando productos para archivo, grabación TV, edición, transferencia o videocámara.

ARCHIVO! Data Media Consumo
EMTEC demuestra estar volcado al mundo multimedia ofreciendo productos dinámicos y siempre a la vanguardia de la tecnología.
CD-R, DVD, TARJETAS DE MEMORIA, - todos los formatos - sean datos, audio, video, imágenes, Emtec tiene el soporte adecuado para cada ocasión.



La empresa EMTEC, productora de soportes para almacenaje de información, lanzará en julio sus nuevos discos DVD-RAM de 4.7 y 9.4 GB. Con estos nuevos productos, que ofrecen unas mayores capacidades de almacenamiento de información, la empresa alemana ofrecerá a todos sus clientes la más amplia oferta dentro de la gama de soportes de almacenamiento digital.
El DVD-RAM es ideal para archivar y editar grandes volúmenes de información por sus posibilidades de acumulación. Fiable y duradero, permite la grabación de datos por las dos caras, proporcionando así una mayor respuesta en cuanto a almacenaje de información. Además, como principal novedad en su utilización, estos dos nuevos modelos incluyen la posibilidad de extraerlos del cartucho en el que vienen protegidos para reproducir la información a través de un DVD-R, duplicando así las formas de acceso a los datos.
Con estos nuevos DVD-RAM, que se han desarrollado en Ludwigshafen, sede central de la compañía, EMTEC cierra, de momento, su gama de productos en el sector del almacenamiento de datos. Junto con los DVD-RAM de 2.6 y 5.2 GB (Type 1) existentes hasta el momento EMTEC ofrece cuatro opciones distintas de capacidad de almacenamiento.

CHINA CENSURA LAS VÍDEOCÁMARAS DIGITALES

China ha aprobado una nueva ley que impone límites y un sistema de censura previa para los vídeos grabados con cámaras digitales, después de que varios documentales de aficionados airearan cuestiones políticamente sensibles.
Las cámaras digitales no estaban hasta ahora incluidas en la lista de tecnologías audiovisuales bajo las leyes de la Administración Estatal que regula la censura en China.
Desde ahora, sin embargo, se prohíbe la emisión de películas digitales sin autorización previa de la autoridad, y se prevén castigos y penas para quienes esquiven el control oficial.
Las minicámaras digitales han causado sensación en el país, donde son utilizadas no sólo por motivos familiares o turísticos, sino también para grabar películas clandestinas, documentales sobre abusos o corrupción e incluso casos de espionaje.



La nota señala que las películas "sobre religión, nacionalidad, y otros temas sensibles deben pedir el consejo (de las autoridades) y recibir aprobación de los departamentos relevantes del gobierno local, antes de ser emitidos". La ley prevé también que las páginas de Internet deberán tener una autorización para permitir bajar vídeos de la Red a los usuarios.

HOT!!

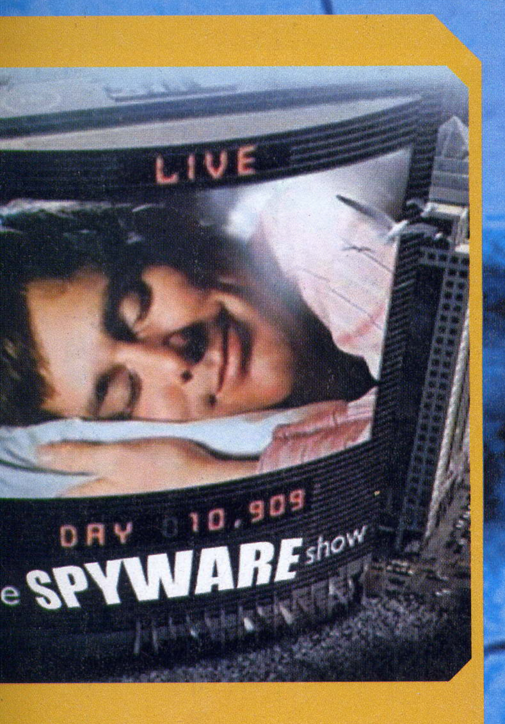
CAMPAÑA CONTRA EL SPAM

La Unión Internacional de Telecomunicaciones (UIT) ha reunido a primeros de junio en Suiza a representantes gubernamentales, proveedores de servicios de Internet, empresas, académicos y organizaciones de consumidores para buscar soluciones contra el correo electrónico comercial no solicitado (spam), que supone, según este organismo, una "amenaza" para la Sociedad de la Información.
Para la UIT, el spam ha pasado a ser "una de las plagas más importantes del mundo digital", con varios "centenares de millones" de e-mails enviados diariamente que amenazan con "obstruir el correo electrónico y los servicios de mensajería móviles e instantáneos".

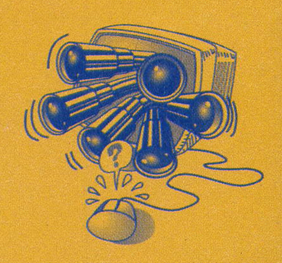
INTERNAUTAS: EL 63% USA EL E-MAIL A DIARIO

Los resultados de la última encuesta del Estudio General de Internet (EGI) muestran que el 19 por ciento de los internautas está conectado permanentemente al correo electrónico, el 18 por ciento se conecta tres o más veces al día; el 10 por ciento, 2 veces y el 16 por ciento, al menos, una vez al día.
Muy alejados de estas cifras quedan el 5 por ciento, que usa el correo electrónico tres o más veces a la semana; el 2 por ciento, que sólo lo utiliza una o dos veces, y el 1 por ciento, que lo utiliza esporádicamente.
Por otra parte, el 13 por ciento de los navegantes en Internet utilizan los foros de discusión (IRC, Chatas, Messenger...) dos o más veces al día y el 8 por ciento, como mínimo, una vez al día.
Otro dato que se extrae de la última encuesta del EGI es que el 7 por ciento de los internautas utiliza estos sistemas de discusión y comunicación online un mínimo de dos o más veces a la semana, el 42 por ciento, como mínimo, una vez a la semana, mientras que un 23 por ciento los utiliza esporádicamente.
Estas cifras indican que la Red se ha convertido en una forma cada vez más integrada en los hábitos de los internautas para relacionarse. Además, EGI señala que está cambiando la forma de relacionarse de los navegantes y que en un futuro éste puede ser el modo usual de comunicarse y entablar relaciones.

Engañar al



Programas espía: si los conoces, los evitas. O sabes cómo liberarte...



Bien, ha pasado. Sabemos que no hay que aceptar software de desconocidos, no hay que pulsar el enlace que promete música (o porno) gratis, no hay que abrir los archivos adjuntos que llegan sin ver quién los manda y en los equipos con riesgo de contagio no hay que usar Windows, sino Linux o Mac OS X. No obstante, se nos ha colado un spyware, que se ha instalado en nuestro PC, que bombardea de publicidad no deseada, comunica nuestros movimientos por el Web a saber a quién e incluso no se deja cancelar. ¿Y ahora? Aún se puede hacer algo...

Bloquear dominios publicitarios

Este truco no requiere ningún programa especial, sólo detectar a qué servidores se conecta el spyware. Para ello podemos usar netstat en el directorio \Windows\. A menudo los programas de adware proporcionan ellos mismos esta información. Para iniciar netstat basta con abrir una ventana del DOS de Windows y escribir el comando netstat. El comando observa la actividad de red del del sistema. Para que sea más cómodo, usamos el comando

```
netstat >> stats.log
```

La actividad de red se guardará en el archivo stat.log, que podremos consultar con calma. El archivo se guarda en el directorio C:\Documents and Settings\User (donde hay que poner el nombre con el que accedemos a Windows en lugar de User). ¡Para quien no lo ha probado antes, es sorprendente descubrir cuánta actividad se produce cuando menos lo esperas! Probamos, por ejemplo, a iniciar un programa de FTP, aún sin conectarse a ningún servidor. Puede ser que netstat se inicie antes o después del programa; basta con hacer algunas pruebas para comprenderlo. Si hay un adware o un spyware activo, normalmente operará por el puerto 1975, cuando por ejemplo un navegador trabajará por el puerto 80, o bien 8080. En el archivo stats.log aparecerá el nombre del dominio al que se conecta el adware. Ahora buscamos un archivo llamado Hosts en el directorio \Windows\. Es el equivalente del archivo /etc/hosts de Unix. En muchos sistemas, incluyendo Windows 2000 y NT, el archivo puede encontrarse en \%SYSTEMROOT%\system32\drivers\etc\.

>> SERVER ADWARE

En http://pgl.yoyo.org/adservers/ aceptan indicaciones de servidores de adware, para recogerlos en una lista negra lo más completa posible, que basta con descargar e insertar en tu propio archivo Hosts para resolver el problema.

```
127.0.0.1   Garden.ngadcenter.net
127.0.0.1   Ogilvy.ngadcenter.net
127.0.0.1   ResponseMedia-ad.flycast.com
127.0.0.1   Suissa-ad.flycast.com
127.0.0.1   UGO.eu-adcenter.net
127.0.0.1   VNU.eu-adcenter.net
127.0.0.1   a32.g.a.yimg.com
127.0.0.1   ad-adex3.flycast.com
127.0.0.1   ad.adsmart.net
127.0.0.1   ad.ca.doubleclick.net
127.0.0.1   ad.de.doubleclick.net
127.0.0.1   ad.doubleclick.net
127.0.0.1   ad.fr.doubleclick.net
127.0.0.1   ad.jp.doubleclick.net
127.0.0.1   ad.linkexchange.com
127.0.0.1   ad.linksynergy.com
127.0.0.1   ad.nl.doubleclick.net
127.0.0.1   ad.no.doubleclick.net
127.0.0.1   ad.preferences.com
127.0.0.1   ad.sma.punto.net
127.0.0.1   ad.uk.doubleclick.net
127.0.0.1   ad.webprovider.com
127.0.0.1   ad08.focalink.com
127.0.0.1   adcontroller.unicast.com
127.0.0.1   adex3.flycast.com
127.0.0.1   adforce.ads.imgis.com
127.0.0.1   adforce.imgis.com
127.0.0.1   adfu.blockstackers.com
127.0.0.1   adimage.blm.net
127.0.0.1   adimages.earthweb.com
127.0.0.1   adimg.egroups.com
127.0.0.1   admedia.xoom.com
127.0.0.1   adpick.switchboard.com
127.0.0.1   adremote.pathfinder.com
127.0.0.1   ads.admaximize.com
127.0.0.1   ads.bfast.com
127.0.0.1   ads.clickhouse.com
127.0.0.1   ads.enliven.com
```

SPYWARE

Si el archivo no existe lo podemos crear. El archivo contiene los dominios incriminados que hemos encontrado con netstat, precedidos por un URL ficticio que hace volver a nuestro equipo. En la práctica el adware creerá que se conecta a su servidor pero en realidad se conectará a nuestro equipo, girando sobre sí mismo:

```
127.0.0.1 spam.com
127.0.0.1 server.spyware.com
127.0.0.1 software.indeseado.com
```

En el ejemplo anterior la dirección 127.0.0.1 es la de loopback, que hace volver al spyware. Los nombres de dominio son inventados y se sustituirán con los encontrados. Si en nuestro equipo hay una función de servidor web, un adware agresivo que insista a llamar a 127.0.0.1 puede ralentizar notablemente el equipo. Por otra parte, este truco no basta para bloquear los adware que se saltan el archivo Hosts y usan un nameserver propio.

Explorer y software de bloqueo

Muchos programas muestran anuncios utilizando los componentes de Internet Explorer. En este caso, basta con configurar en Explorer como proxy de la conexión un URL que bloquee los mensajes publicitarios no deseados. El mismo truco vale con programas de bloqueo y filtro. Algunos programas, como los cortafuegos, pueden prohibir el acceso a Internet programa por programa.

Spoofer y DLL falsa

Otro truco antispyware es hacer creer a los progrmas publicitarios que todo funciona. En realidad hablan con otro programa, presente en nuestro equipo, que finge ser su servidor de referencia. Puede no ser ni siquiera un programa, sino sólo componentes falsos, que cuando son interrogados por el spyware responden valores creíbles pero inocuos. Un programa típico para este uso es SpyBlocker (http://noads.hypermart.net/). En http://www.cexx.org/dummies.htm hay una lista de archivos falsos. Se llaman como ciertos componentes de spyware y contienen lo necesario para pasar la prueba. Pero no abren ninguna conexión a Internet.

list ad server hostnames: [as a browser proxy autoconfig file] with [links back to this page]
only show entries added since:* [ ] [ ] [ ] view list as plain text: [ ] [go]

list ad server IP addresses: [as a browser proxy autoconfig file] with [links back to this page]
view list as plain text: [ ] [go]

* leave the date blank to list all entries. if one or more fields is set, today's date is used for any unset fields.

Un remedio radical

¿Por qué no borrar simplemente los archivos del programa adware? Esto funciona sólo cuando el programa presupone que los usuarios no saben siquiera aislar archivos con nombre reveladores como advert.dll, ad.dll, adserver.dll y otros. Se puede probar, sin preocuparse más. Tal vez el programa que transporta el spyware siga funcionando y, si no funciona, puede recuperar el archivo borrado. A menudo el programa sigue funcionando, pero el spyware muere. ¡Bingo!

Vamos al editor

Otra alternativa posible es el uso de uneditor de recursos, con el cual se modifican o borran recursos como las ventanas publicitarias. Un buen editor es Resource Hacker (http://www.rpi.net.au/%7Eajohnson/resourcehacker/).

Fuera del registro

A menudo el adware modifica el registro del sistema de Windows o inserta cosas en la carpeta Startup, de modo que al arrancar el equipo el adware también se cargue inmediatamente. Es difícil borrar este tipo de modificaciones y a menudo el programa portador del adware se apresura a resintalarlo en cuanto empecemos a utilizarlo.

Algunas versiones de Windows disponen de un programa llamado MSCONFIG que permite visualizar y deshabilitar las aplicaciones de Inicio. MSCONFIG se ejecuta mediante Inicio -> Ejecutar, seguido del nombre del programa (msconfig).

127.0.0.1	ads.fairfax.com.au	127.0.0.1	ads.ninemsn.com.au	127.0.0.1	ads03.focalink.com	127.0.0.1	ads17.focalink.com
127.0.0.1	ads.fool.com	127.0.0.1	ads.seattletimes.com	127.0.0.1	ads04.focalink.com	127.0.0.1	ads18.focalink.com
127.0.0.1	ads.freshmeat.net	127.0.0.1	ads.smartclicks.com	127.0.0.1	ads05.focalink.com	127.0.0.1	ads19.focalink.com
127.0.0.1	ads.hollywood.com	127.0.0.1	ads.smartclicks.net	127.0.0.1	ads06.focalink.com	127.0.0.1	ads2.zdnet.com
127.0.0.1	ads.i33.com	127.0.0.1	ads.sptimes.com	127.0.0.1	ads08.focalink.com	127.0.0.1	ads20.focalink.com
127.0.0.1	ads.infi.net	127.0.0.1	ads.tripod.com	127.0.0.1	ads09.focalink.com	127.0.0.1	ads21.focalink.com
127.0.0.1	ads.jwtt3.com	127.0.0.1	ads.web.aol.com	127.0.0.1	ads1.activeagent.at	127.0.0.1	ads22.focalink.com
127.0.0.1	ads.link4ads.com	127.0.0.1	ads.x10.com	127.0.0.1	ads10.focalink.com	127.0.0.1	ads23.focalink.com
127.0.0.1	ads.lycos.com	127.0.0.1	ads.xtra.co.nz	127.0.0.1	ads11.focalink.com	127.0.0.1	ads24.focalink.com
127.0.0.1	ads.madison.com	127.0.0.1	ads.zdnet.com	127.0.0.1	ads12.focalink.com	127.0.0.1	ads25.focalink.com
127.0.0.1	ads.mediaodyssey.com	127.0.0.1	ads01.focalink.com	127.0.0.1	ads14.focalink.com	127.0.0.1	ads3.zdnet.com
127.0.0.1	ads.msn.com	127.0.0.1	ads02.focalink.com	127.0.0.1	ads16.focalink.com	127.0.0.1	ads3.zdnet.com



¡DESCUBRE LOS SERVIDORES PINCHADOS!

Cómo probar la seguridad de un servidor Web en pocos minutos con un buen software de escaneo, como Shadow Security Scanner. Recuerda: ¡no abuses!

La cantidad de software disponible hoy en la red para quien necesite reparar un servidor es muy elevada. A veces, también lo es la calidad.

Shadow Security Scanner es un escáner de red capaz (como tantos otros productos análogos) de encontrar todos los servicios activos en un host, efectuar una serie de pruebas en ellos y proporcionar un cómodo informe en el que se listan todos los posibles fallos presentes en el sistema junto con las soluciones a implementar y varios enlaces a los que acudir para obtener información detallada sobre cualquier vulnerabilidad detectada.

Como hemos dicho, existen en el comercio otros muchos programas que hacen más o menos lo mismo: sin salir del entorno Windows, por ejemplo, el más famoso (y uno de los más caros) es sin duda Retina; y recientemente la propia Microsoft ha lanzado su propio escáner de seguridad. Linux es el territorio del celebérrimo SATAN, SAINT, y del indiscutible Nessus.

Shadows Security Scanner se presenta como un paquete instalable de 7 MB, descargable en versión shareware del sitio de su programador (Red Shadow) www.safety-lab.com: si en sus primeras versiones SSS era probablemente poco más que una buena herramienta escrita por un apasionado del hacking (en efecto, el programa tenía una pinta muy "black hat" incluso en los gráficos) el éxito que ha obtenido ha empujado a sus creadores a darle un tono decididamente más profesional y "business oriented".

La interfaz es clara y eficaz (van por la versión 6.98), la instalación no presenta más dificultad que pulsar "next" en cada paso del asistente, al igual que su uso, de lo más simple: para uno uso básico no es preciso más que insertar el host a escanear y pulsar sobre "start".

Hecho esto, el escáner empieza a hacer pings al host, efectúa conexiones por un amplio conjunto de puertos remotos y empieza a recabar información.

En la segunda fase de la prueba se implementarán todos los diversos intentos de exploiting, password cracking y compañía que al terminar el escaneo llevarán a obtener un detallado informe (con muchos gráficos inútiles, tan importantes para los agentes comerciales que viajan vendiendo "seguridad" en forma de informes generados en 5 minutos de software así...)

Por cada "audit" encontrado (es decir, cada posible fallo) tendremos una descripción del problema y un posible test a efectuar al final para verificar sin lugar a dudas si nuestro equipo está realmente afectado por ese tipo de problema: si por ejemplo se detecta el infausto "unicode transversal bug" encontraremos en el informe un url formado a propósito para mostrar cómo es posible ejecutar comandos remotamente en nuestro servidor, o si por ejemplo se descubre una versión con fallos de un servidor FTP encontraremos un enlace a la base de datos de securityfocus que nos llevará al problema en cuestión.

Además, está presente también una descripción de los procesos a implementar para corregir la vulnerabilidad encontrada; en algunos casos, como por ejemplo cuando la solución a un bug hace necesario sólo modificar el registro del sistema, es posible corregir el error simplemente pulsando un botón rotulado "Fix-it", si bien se nos advierte de que no siempre este procedimiento es eficaz. Adentrándonos un poco más profundamente entre las diversas opciones que SSS ofrece, sin embargo, empezamos a encontrar varias cosas que lo hacen más interesante: es posible editar las políticas que utilizará el motor del programa para efectuar el escaneo y aplicarlas en combinación con una host-list.

HAY QUIEN VENDE "SEGURIDAD" Y SIN EMBARGO USA SOFTWARE PARECIDO A ÉSTE, NADA MÁS.

Si por ejemplo en nuestra red están presentes dos servidores, uno Linux y otro NT, podremos decir a SSS que en el primero se efectúen controles sobre servicios típicos de equipos Linux, mientras que en el segundo solo aquellos proclives a contener fallos en NT. El ahorro de tiempo es notable. Podemos también planificar el escaneo (para efectuar quizá notas o en condiciones previstas de poco tráfico en la red) y efectuar pruebas específicas por lo que respecta al denial of services y password cracking (están presentes herramientas dedicadas para estas operaciones).

>> Siempre al día

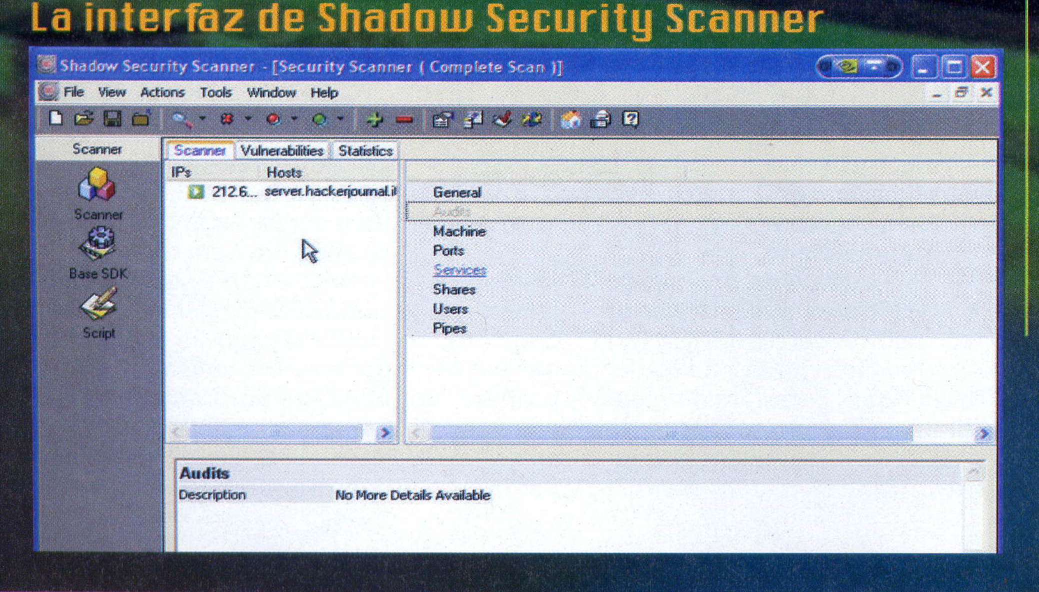
Respecto a la actualización de la base de datos de vulnerabilidades, incluso esto es una operación de lo más simple con un update automático que descargará las actualizaciones y las instalará en pocos minutos.
En suma, en sus últimas revisiones SSS se ha orientado claramente hacia el aspecto de uso que requiere un porgrama simple de utilizar y que sea al menos medianamente fiable.
Está claro que ningún software podrá sustituir nunca el consejo de un experto, y muy a menudo en los informes se señalan falsos positivos que normalmente se limitan a intervenir para verificar que todo esté bien.
También es cierto que este programa, por su diseño y por lo que ofrece, funciona bien: muy atentido por sus programadores, se actualiza a menudo y mejora en diversos aspectos continuamente, y actualmente es una solución económica (la licencia cuesta 200 Euros) para pequeñas empresas que no pueden permitirse un responsable de seguridad y que a través de SSS tienen la oportunidad al menos de "tapar" los agujeros más clamorosos.
Con la frecuencia con que encontramos navegando por la red empresas que albergan 250 sitios web comerciales y que no han aplicado jamás al servidor un Service Pack para NT 4.0, es sin duda positiva la difusión y el uso de software de este tipo.
¿Es sensato fiarse de SSS para la seguridad de nuestro servidor? Ante su bajo coste (Retina ofrece más, es cierto, pero cuesta 100 veces más), y teniendo en cuenta que nunca se podrán obtener resultados comparables a los que sólo un experto humano puede garantizar, es cuando menos recomendable probar la versión shereware, válida durante 15 días, y hacer un par de pruebas en el servidor web: la cantidad de "rojo" presente en el monitor será el mejor índice de consulta. Hay que tener presente que existen otros muchos productos, algunos de los cuales son gratuitos como Nessus para Linux, que es claramente superior a SSS en muchos aspectos (arquitectura cliente-servidor, versatilidad, etc.) pero que probablemente se dirigen a otro tipo de uso, dada su relativa complejidad.
Instrumentos como Shadow Security Scanner sin duda no es la varita mágica con la que convertir en seguro un servidor web, pero hace posible para quien no puede permitirse un experto en seguridad informática poder salir a la red con riesgos de seguridad claramente inferiores respecto a quien se limita a instalar NT y a remojarse los pies en las aguas infestadas de la red.



>> El libre albedrío

La otra cara de la moneda es el uso destructivo que es posible hacer de programas como éste: de hecho, podemos escanear cualquier host, obteniendo mucha información sobre el sistema operativo y sobre los servicios instalados; y es probablemente verdad que muchos kiddies encuentran en ellos un instrumento bastante potente que les proporciona url de información para poder ejecutar comandos en un servidor con un simple clic. Pero el discurso es siempre el mismo: no se trata nunca de evaluar si un instrumento es de por sí bueno o malo. Bueno o malo será siempre y sólo el uso que se haga de él.

La interfaz de Shadow Security Scanner



◁ *Unos clics y pocos conocimientos básicos para probar cualquier host.*

Una llamada de 10



"Hola, soy Mike Hansen de moneda extranjera del National Bank de Los Angeles, buenos días" ¿Podemos estar seguros? ¿Y si es un impostor que quiere robar información? ¿Y si fuera... un ingeniero social?

THE INSURANCE INSTITUTE OF LONDON{PRIVATE }



"INTERNET CRIME"

BY

OLIVER PRIOR

(Research Development and Knowledge Management, Willis)

Stanley Mark Rifkin, un atento trabajador empleado en una empresa de software. 32 años bien llevados, de inteligencia aguda, óptima capacidad técnica y, ante todo, una curiosidad infinita. El año de autos: 1978. El lugar donde ocurre todo: Los Angeles. Ahora ya no existe, pero antes, cerca del centro de Los Angeles, se levantaba un gran palacio que albergaba el Security Pacific National Bank. Rifkin tenía acceso a las áreas limitadas del edificio porque era encargado de la configuración de un sistema de backup de los datos del ordenador central del banco. Un trabajo intrigante y delicado. Rifkin no se hacía notar, como los empleados de todo el mundo poco atentos a la seguridad de los datos reservados, preparaba cada mañana una nota donde escribía los códigos que había que usar en la sala de télex, es decir, el código de confirmación de cualquier operación bancaria. Cada un día un código distinto, naturalmente. Cuestión de seguridad, naturalmente... No es difícil imaginar cómo en aquella sala transitaban millones de dólares, cada noche, todos los días, en el cierre de las operaciones.

Rifkin, con la astucia que desde luego no le faltaba, consiguió echar un vistazo al código en la nota, dejada a la vista de todos, y así fue como le vino la idea de estudiar una estrategia de ataque.

¿Por qué tendría que aprender sofisticadas técnicas de hacking, cuando basta una llamada?

¿Por qué motivo, se preguntó, tendría que aprender técnicas de hacking o descargar utilidades de ataque de la Red dedicando días y largas noches por Internet, cuando basta una llamada para aumentar la propia cuenta bancaria con, digamos, 10 millones de dólares? Una pregunta aparentemente ingenua, o extraña, tal vez sin fundamento, que sin embargo es el punto de partida del ingenioso mecanismo. O, si se prefiere, de la puesta en práctica de una actividad de ingeniería social. No es preciso graduarse para ser un ingeniero social: basta con una gran curiosidad, una alta

MILLONES de dólares

capacidad de persuasión, sangre fría, coraje, y una buena dosis de "verborrea" y de habilidad en la gestión de relaciones con otras personas.

El ataque

Aquí es donde entra en acción Rifkin, alias Mike Hansen, de moneda extranjera del banco. Desde un teléfono del propio edificio del Security Pacific National Bank, abre una cuenta del Wozchod Bank de Zurich. La táctica era lo más simple posible, al menos en teoría. Así, a primeros de octubre, observó a un empleado al que conocía bien y obtuvo de él fácilmente el código de acceso a lo que había bautizado mentalmente como 'la sala del tesoro'. Con el código y mucha cara dura, se introdujo en la sala de télex con la excusa de un control del software del host central. Enviar una orden ya preparada de transferencia de la sede central a su cuenta suiza, por una cifra cercana a 10.200.000 dólares, se resolvió con la pulsación de sus sudadas manos de unos pocos números.

Se confirmó la transferencia. Pocos días después Rifkin voló a Suiza para sacar su dinerillo, que en gran parte utilizó para comprar diamantes (que por otra parte, el banco tenía dificultades en vender para recuperar al menos en parte el dinero sustraído).

Una vez descubierto, Rifkin entró en el guinnes de los récords: había completado uno de los mayores robos bancarios sin usar pistola ni ordenador: sólo un teléfono. Lo sorprendente es que esta operación se considera de puro hacking, tanto que sólo se ve sobrepasado por, sorpresa, un tal Kevin D.Mitnick.
Una sorpresa comprensible: una operación así, surgida de la escrupulosa planificación de una actividad de ingeniería social bien conocida por cualquier hacker, se ha completado con la consecución de un interés propio: en esto el hacking no tiene nada que ver. La fama, tal vez, proviene solamente de la morbosa participación que todos tenemos ante la inteligencia aplicada, contra la estupidez rutinaria de quien, por el contrario, debería estar siempre alerta.

El falso sentido de seguridad

La información reservada estaba a su alcance, le bastaba sólo coraje y sangre fría en cantidad

Es evidente que nuestro sentido de la seguridad está demasiado vinculado sólo a los instrumentos informáticos. De acuerdo, existen hoy en el mercado imponentes programas de defensa que permiten garantizar un adecuado nivel de protección de datos, pero el hombre siempre acaba siendo el eslabón débil de la cadena. Ante instrumentos de cifrado, software para el control de acceso, instrumentos de autenticación y todo lo demás, un hacker hábil puede, por un momento, dejar de lado el ordenador y entrar por la puerta grande, colándose de rondón.





PIRATAS CHINOS

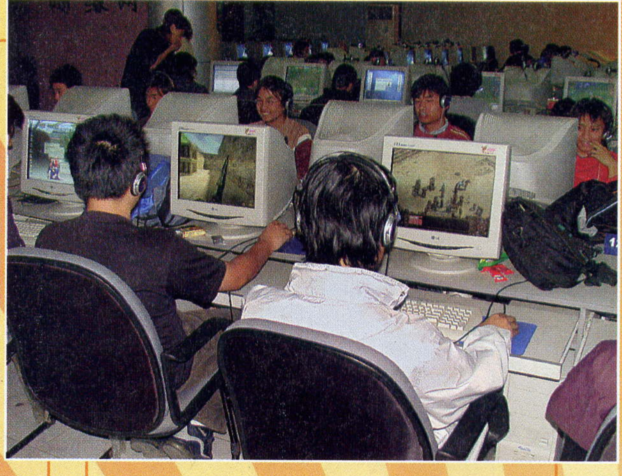
Nacionalistas, instrumentalizados, pero románticos.

"Este país es nuestro país, este pueblo es nuestro pueblo; si no gritamos, ¿quién lo hará? Si no actuamos, ¿quién actuará?" Inscrito en la página de bienvenida del primer sitio de los Hongke, los hackers chinos más activos, este eslogan de Mao Tsé Tung resume una de las tendencias más pronunciadas de los piratas de Internet del gran país: una implicación política con una fuerte connotación nacionalista.

>> Hackers, amigos o enemigos del gobierno

El gobierno chino ha tardado mucho en tomar medidas contra los ataques de hackers. No fue hasta agosto de 2000 cuando Xu Rongsheng, representante de China en el grupo de trabajo sobre las redes de la UNESCO, obtuvo luz verde para la creación de la primera fuerza anti-hackers china. Con una docena de miembros, intenta proteger los sitios oficiales chinos, y especialmente los de las instituciones financieras, contra toda forma de piratería.
En septiembre de 2001, Wang Qun, un estudiante originario del centro de China, sufrió en sus propias carnes la eficacia de esta pequeña unidad anti-hackers. Fue detenido tras haber reemplazado las páginas de bienvenida de departamentos ministeriales locales por imágenes eróticas. Pero las autoridades chinas parecen por el contrario mucho más indulgentes con los hackers nacionalistas que atacan sitios americanos o japoneses en períodos de tensiones diplomáticas. Así, la Hongkers Union of China, el grupo de hackers más comprometido políticamente, parece tener las puertas abiertas para llevar a cabo sus ataques. Una impunidad que hace suponer un soporte implícito por parte del gobierno chino.

Aparecidos a mediados de los años 90, los primeros hackers chinos llevan un importante retraso tecnológico respecto a sus homólogos americanos o europeos. Los ordenadores están aún poco extendidos, el acceso a Internet sigue siendo un lujo, y los primeros internautas se limitan a intercambiar ideas en BBS, un sistema de mensajería aún muy popular actualmente. Los hackers, que aún tiene mucho que aprender, se inician en las tecnologías de la red pirateando los programas y software extranjeros.
Un suceso de política internacional precipitará la cohesión de los hackers chinos. En 1998, amotinados xenófobos agitan Indonesia: tomada como rehén, la comunidad china del país es víctima de violencia, sus almacenes son presa del pillaje, sus casas son expoliadas a sangre y fuego. Estos amotinados provocan la emoción de los chinos, que en su mayor parte se sienten totalmente impotentes. Pero los hackers se dan cuenta de que tienen los medios para actuar. Con una tecnología limitada pero una voluntad inquebrantable, inundan los buzones de correo de los sitios del gobierno indonesio, paralizando muchos de ellos. La primera "ciberguerra de protección de la patria", según los términos de los propios hackers chinos, pone las bases de la organización de los diferentes movimientos del país.
En chino, hackers se dice "hei ke", literalmente "pasajero negro", un color que, en



China, simboliza la ilegalidad. Las diversas asociaciones creadas en el país han declinado, pues, toda una paleta de colores para afirmar sus diferencias. Tras la primera ciberguerra, empiezan a dibujarse tres tendencias. Los Hongke, muy politizados, son los "pasajeros rojos": se trata de la asociación más influyente del país, y de la quinta agrupación de hackers del mundo. Extremadamente nacionalistas, los Hongke están en el origen de seis ciberguerras, y están bajo una fuerte sospecha de recibir soporte,

维护中国网络安全的精锐之军

中国黑客第一军团



al menos tácito, del gobierno chino. Crearon su primer sitio de Internet al día siguiente del bombardeo de la embajada de China en Belgrado, en abril de 1999, y tuvieron un éxito inmediato: sus páginas recibieron 500 000 visitas en pocos días. En abril de 2001, tras la colisión entre un avión de reconocimiento americano y un jet chino, 80 000 personas participaron en los ataques a sitios americanos orquestados por Hongke. Banderas chinas flotan durante algunos días en las páginas de bienvenida de ciertas administraciones americanas, acompañadas de eslogans nacionalistas como "preservemos la soberanía nacional", "deshonra para quienes no resistan", o bien "ataquemos la arrogancia antichina".

Más pacifistas, los Lanke, "pasajeros azules", se concentran en las cuestiones tecnológicas y los desafíos de seguridad de la red. En cuanto a la "armada verde", franqueó muy pronto el paso de la comercialización: sus cinco fundadores crearon en julio de 1999 una empresa que trabaja en la seguridad de redes informáticas. Actualmente cuenta con una plantilla de unas sesenta personas.

Y es que entre dos ciberguerras, los hackers chinos se han aplicado a recuperar su retraso tecnológico inicial. En 1998, pusieron a punto su primer programa "caballo de Troya", llamado Netspy. El aumento de potencia tecnológica de los hackers chinos comporta el desarrollo de sistemas de protección cada vez más sofisticados. En octubre de 2000, una empresa de Cantón puso a punto un cortafuegos llamado "Blue Shield", que fue reconocido por el Ministerio de seguridad pública como el primer sistema defensivo completamente chino. Otra empresa comercializó al mismo tiempo el programa "hacker killer ", el más utilizado actualmente en China, capaz de contener unos ochocientos métodos de pirateo informático. "Los hackers han aportado mucho a la red china, demostrando sus problemas de seguridad, e inventando programas de seguridad", afirma uno de ellos.



Militantes políticos nacionalistas o pequeños genios de la tecnología, los hackers chinos tienen que trabajar duro cada día para preservar su independencia frente a las autoridades locales. Y siguen conservando una concepción muy romántica de su función, como se ilustra en esta firma lírica de Hacker X Files, una de las revistas informáticas especializadas: "en realidad, un psiquiatra es también un hacker, un hacker que rompe el alma de la gente. Pero nosotros salvamos a la gente, hermano...".

>> El cebo libertario de Internet en China

Internet puede ser un instrumento de doble filo en la China popular. Los 470 000 sitios chinos ofrecen a los internautas una formidable ventana al mundo, que consigue compensar el control drástico de la información ejercido sobre los demás medios locales. Pero los 68 millones de internautas chinos, de los que el 80% tiene menos de 24 años, se han dejado engañar en ocasiones por esta aparente libertad del web: según un informe de Periodistas sin fronteras, publicado en junio de 2003, China detenta el triste récord del número de ciberdisidentes en la cárcel. 42 personas, rastreadas por la ciberpolicía china, pasan de 3 a 15 años de cárcel por haber publicado en la red información contraria a los intereses del gobierno.

Éste ejerce además un control drástico sobre Internet, bloqueando los sitios de contenido político sensible: por ejemplo, es imposible, acceder directamente desde Pekín a las páginas de Amnistía Internacional o de los tibetanos en el exilio. Incluso los buzones de correo pueden ser objeto de censura gubernamental.

Como un CUBO

NADIE LO PIENSA, pero de un disco duro abandonado en la basura se encuentra de todo, y el vecino de al lado puede ponerse a espiar en la basura.

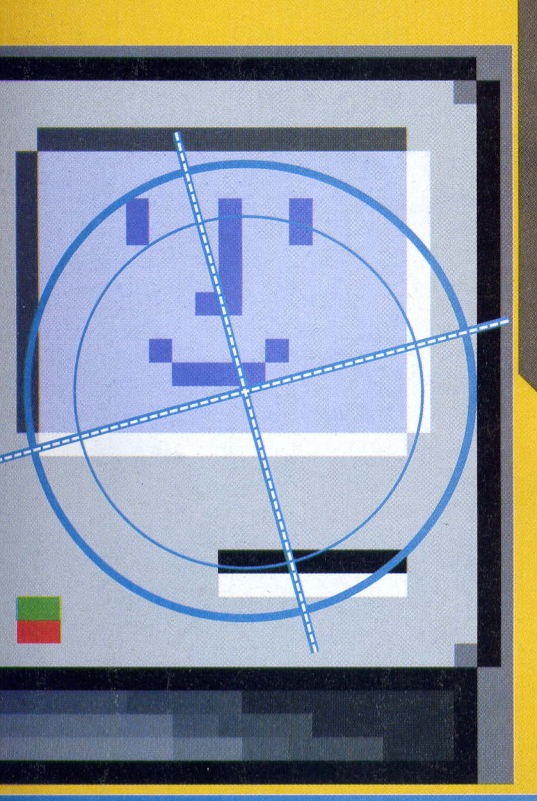


En América los hackers de antes husmeaban de noche en los deshechos de las empresas en busca de números de servicio para llamar gratis. Hoy en los contenedores se encuentra algo mucho más precioso: los discos duros.

Hace tiempo, Simson Garfinkel (http://simson.net/blog/), periodista técnico americano, llevó a cabo una investigación, buscando discos duros en la basura, y comprando viejos discos usados en los mercadillos y hasta en el Web. De los discos tirados o comprados de segunda y tercera mano recabó más de cinco mil números de tarjeta de crédito, informes médicos, información familiar y financiera, varios gigabytes de correo electrónico y archivos pronográficos pertenecientes a los anteriores propietarios de los discos en cuestión.

> Qualquiera podría abrirlo, tomar el disco duro y hurgar en su interior...

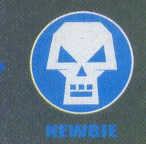
Según Dataquest, en 2001 quedaron fuera de servicio más de 130 millones de discos duros en todo el mundo, y 150 millones en 2002.



PROGRAMAS BORRALOTODO

Estos son algunos programas proyectados para destruir los viejos datos para siempre:

- **CyberScrub**
  http://www.cyberscrub.com/
  De pago (39.95 dólares), demo 15 días
- **Data Scrubber Hard Drive Degaussing Software** http://www.datadev.com/ds100.html
  ¡1.995 dólares!
- **Eraser**
  http://www.heidi.ie/eraser/
  Donateware (15 dólares)
- **UniShred Pro**
  http://www.lat.com/
  De pago (también para Linux, 450 dólares)
- **WipeDrive**
  http://www.accessdata.com/Product07_Overview.htm 39,95 dólares
- **Wipe:** http://wipe.sourceforge.net/
  Gratis, también para Linux



de la BASURA

DESPROTEGIDOS POR LA LEY

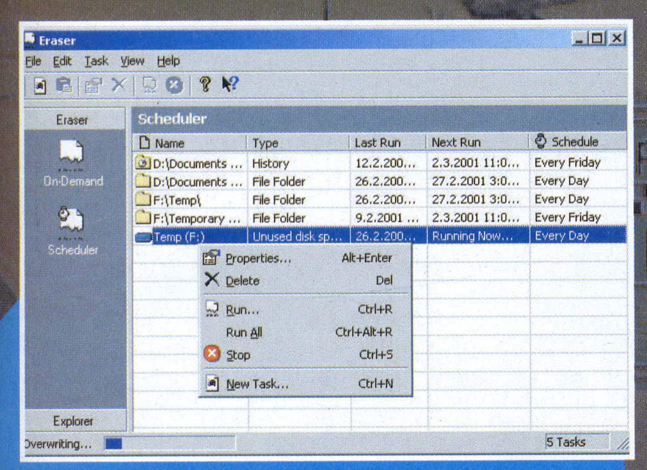
Hay casos y casos, pero en general no se tiene derecho a la privacidad sobre datos que se han tirado a la basura. Así, quien andase hurgando en nuestro viejo disco duro podría no correr riesgos.



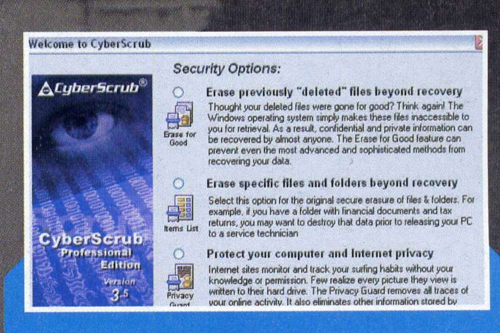
¿Has borrado los datos del disco duro del viejo PC antes de tirarlo?

De 158 discos duros comprados a precio de saldo, 129 aún funcionaban. 28 de ellos conservaban datos sin cifrar, sin que nadie se hubiera preocupado de borrar nada. En uno de los discos incluso estaba el registro de un año de transacciones financieras: formaba parte de la contabilidad de una empresa.

También donde los datos habían sido borrados, en la mayor parte de los casos un simple comando Undelete junto con programas de reparación, como las Norton Utilities, sacaron a flote gran cantidad de datos. La mayor parte de la gente piensa que basta con borrar un archivo para eliminarlo de la faz de la tierra; sin embargo, el archivo es ignorado por el PC, que considera libre el espacio que ocupaba, pero lo deja donde está. De todos los discos, sólo doce habían sido limpiados adecuadamente, sin que fuera posible recuperar nada. Incluso un nuevo formateo es un proceso completamente seguro. Las agencias superprofesionales aseguran que pueden recuperar un archivo sobreescrito en el disco hasta siete u ocho veces. Ello significa que, si queremos librarnos de modo realmente definitivo de los datos presentes en nuestro viejo disco duro, borrarlo o reformatear una sola vez no bastará. Un buen procedimiento consiste en reformatearlo al menos diez veces y luego destruir físicamente el disco, haciéndolo pedazos demasiado pequeños como para que sea posible recabar nada (¡si los pedazos son demasiado grandes aún hay posibilidades!) Es una paradoja; ¿cuántas veces ocurre que es definitivamente fácil perder datos valiosos? Y sin embargo librarse de ellos para siempre, con el 100% de certeza, es realmente mucho más difícil. ■



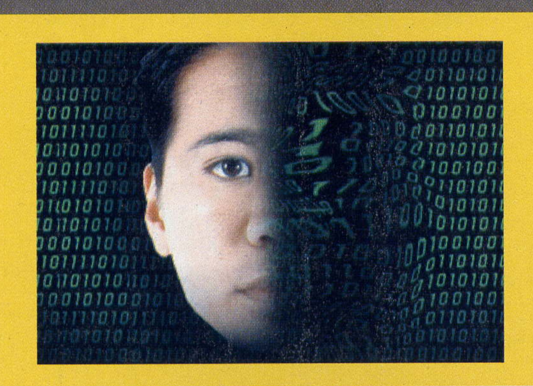
↗ *Eraser promete borrar completamente los datos sensibles y es gratis. Ahora bien, a quien lo usa se le exhorta a pagar 15 dólares, en la lógica del donateware.*



↗ *CyberScrub es una de tantas herramientas que ayudan a destruir de forma definitiva y segura los archivos confidenciales.*

LADRONES DE IDENTIDAD

Según un estudio encargado por la Federal Trade Commission de Estados Unidos, más de un norteamericano de cada veinticinco ha sufrido durante el año pasado un robo de identidad, desde leve –como puede ser un abono no deseado a un sitio porno, efectuado por alguien que ha robado un número de tarjeta de crédito– hasta gravísimo, con la total apropiación de una identidad por parte de alguien malintencionado. En los últimos cinco años, le ha ocurrido a un norteamericano de cada diez. El daño económico se calcula sobre cerca de diez mil dólares por víctima, con un total de treinta y tres millardos de dólares durante el año pasado. En España las cifras son indudablemente inferiores, pero para ninguna de las víctimas de nuestro país esto resulta especialmente reconfortante.



Microsoft es TIRAR el dinero

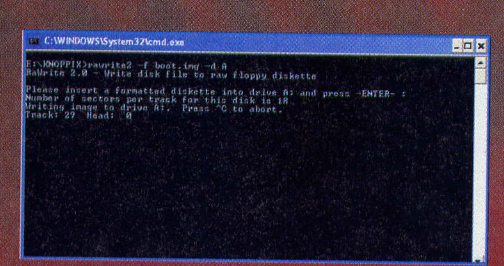
Damos un directo al hígado de Bill y nos procuramos un simple CD: el de Knoppix. Ahorramos casi 700 euros: precio medio de Windows + Office. Porque Knoppix, de hecho, no es sólo Linux, además contiene todo el software necesario para sustiruir los programas de Microsoft. ¡Gratis!

Muchos conocen ya Linux-Knoppix, pero debido al interés que despierta y a ciertas dificultades que suelen encontrarse en los sitios 'mirror' desde donde descargar el software, creemos que vale la pena decir algo más. Esta instalación de Linux es de la serie Live CD, por lo que no requiere efectuar ninguna partición en particular en el disco duro del equipo. Todo se carga directamente del CD.

Cómo descargarlo

El CD viene lleno y, por ello, tendremos que descargar de la red unos 700 MB de software. Una gran ocasión para pasarse al ADSL, o visitar al vecino que lo acaba de instalar. El sitio de partida en busca del archivo correcto es www.knoppix.com, luego un clic sobre requirements para ver si nuestro pc es adecuado (aunque seguro que lo és, ni que sea un poco antiguo), y luego un clic sobre download.

Aparece una larga lista de mirrors, o sea, de todos los servidores dispersos por el mundo donde se encuentra una copia fiel, en teoría idéntica, del servidor principal que contiene Knoppix. Elegimos el archivo KNOPPIX_V3.3-2003-11-19-EN.iso.



△ *Arrancamos mkfloppy.bat del CD tostado y preparamos un floppy de arranque.*

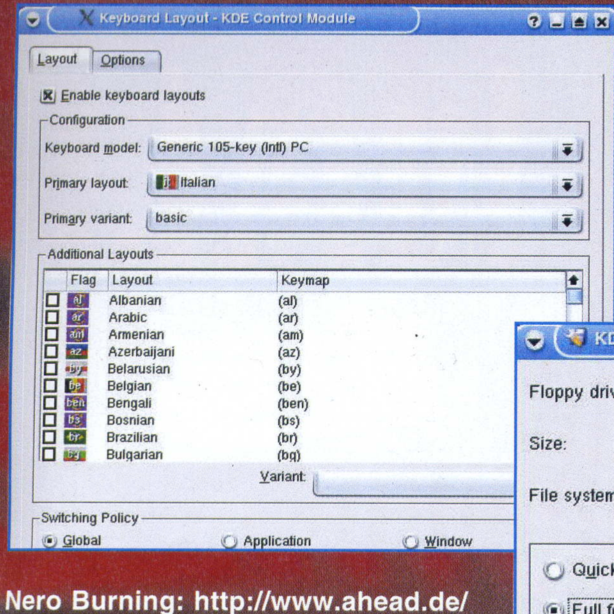
Descargando en el filo de la conexión

Lo confesamos: es cuestión de suerte. En dos de tres casos hemos experimentado la superación del 90% de los bytes recibidos y hemos vista interrumpida la conexión con el servidor, por algún motivo totalmente desconocido. Tanto con sitios de aquí como de lejos. Un tercer intento en sitios holandeses nos ha permitido descargarlo todo, y velozmente.

Para obviar estos inconvenientes puedes probar a usar GetRight (http://www.getright.com) o Go!Zilla (www.gozilla.com), dos gestores de download que lo recuperan en caso de problemas. Si consigues terminar y tu Windows tiene ya instalado un programa para tostar CD (Windows sirve aún para algo...), verás como se inicia automáticamente una sesión de burning: inserta un CD en blanco y ya está listo.

Si Windows no ha instalado un software de tostado de CD, habrás descargado un enorme archivo .iso. ¿Qué hacer con él? Ante todo tendrás que instalar un programa de masterizado. Puedes elegir descargar de la red uno de estos:





◁ *Una de las primeras cosas que hay que hacer es un clic secundario sobre la banera abajo a la derecha para configurar el teclado.*

▽ *Para formatear los floppy que necesitemos utilizamos Kfloppy.*

Nero Burning: http://www.ahead.de/en/index.html, es el más famoso, está en versión de prueba, y es totalmente funcional;
Burn4Free: http://www.burn4free.com/ que tiene la ventaja de ser freeware y de paso permite iniciar desde archivos .iso; así se masteriza el CD.
Al terminar la masterización, el autorranque del CD abre una página html que se abre en el navegador, indicando que el trabajo está hecho.

Siempre encima: es la divisa del hacker

La página está también en español (ES). La leemos de arriba abajo y habremos llegado a la mitad del camino. Para arrancar Linux en nuestro PC tendremos dos posibilidades: activar el bootstrap desde el CD o crear un floppy de boot. Para evitar cualquier inconveniente recomendamos la creación de un floppy. Así, junto con el otro, podremos arrancar con Linux en cualquier equipo, llevando encima solamente la suite compuesta por el CD y el floppy.
Vayamos donde vayamos, los dejaremos estupefactos: verán que podemos iniciar Linux en su propio equipo sin hacer nada más que insertar los dos discos. ¡No hay que menospreciar las ocasiones para crearse una leyenda!

"Sorprenderemos a los amigos arrancando Linux en su propio equipo sin tocar nada más"

Cómo crear el floppy de boot

Preparamos un floppy formateado y lo insertamos en el lector A:. Abrimos el CD (con el Explorador de Windows) y entramos en el directorio KNOPPIX. Dos clics sobre el archivo mkfloppy.bat y tras unos minutos tendremos listo el floppy de boot. ¡No puede ser más simple!
Ya que estamos puestos, leemos también KNOPPIX-FAQ-ES.txt que contiene una serie de respuestas a preguntas habituales y a las dudas más frecuentes.

¡Linux!

Reiniamos el equipo con el CD y el floppy ambos insertados en sus lectores. Tras el inicio con la pantalla tipo terminal, aparece una interfaz KDE que, si no hemos utilizado nunca antes Linux, nos dejará sin duda alguna con la boca abierta. Una organización gráfica con iconos y carpetas, el menú desplegable que se usa para lanzar las aplicaciones, los subdirectorios accesibles con los menús en cascada te darán la sensación de saberlo utilizar ya todo. Y en parte es verdad.
En el escritorio se representan los volúmenes presentes en el pc, incluido también el volumen del disco duro que utilizamos normalmente. Dentro, todos nuestros documentos en modalidad de sólo lectura, para evitar que estropeemos algo.

La desventaja

Obviamente, la desventaja del método Live CD es que la configuración inicial del sistema no prevé el montaje de soporte de memoria masiva ya formateada por sistemas operativos distintos. Por ello, en un principio, sólo podremos guardar archivos de datos basándonos de momento en la home (que de hecho es la RAM) o guardando en el disquete.
También la configuración se perderá, si no la guardamos con la utilidad adecuadda que se encuentra en:

Start Applications>Knoppix>Configure>Save Knoppix Configuration

Si tenemos que formatear un disquete, utilizaremos:

Start Applications>Utilities>KFloppy

Pero la primera operación que conviene hacer es cambiar la configuración del teclado al español:

Clic Secundario sobre la bandera>Configure>Primary Layout

La guinda

Finalmente, para empezar a trabajar en serio, vamos a utilizar el paquete Office (Word, Excel... ¿te suenan estos nombres? :-)

Start> OpenOffice.org 1.1.0

Los programas se disponen al trabajo en un tiempo relativamente menor que un arranque normal de Word y podremos guardar texto y datos en muchos formatos, incluidos los de Microsoft .
Estamos usando Linux y una larga lista de aplicaciones sin arruinarnos, gastando 1 euro por el CD. Es todo.

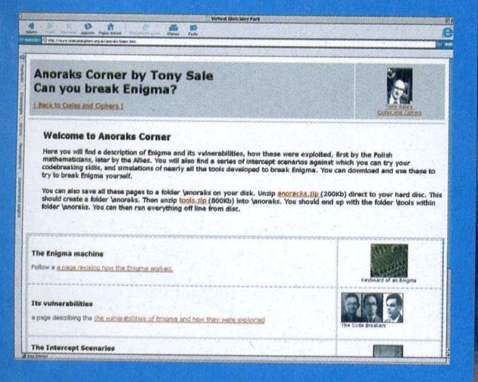
CÓDIGO NAZI:

La máquina que generaba los *códigos secretos* para los nazis en la Segunda guerra mundial



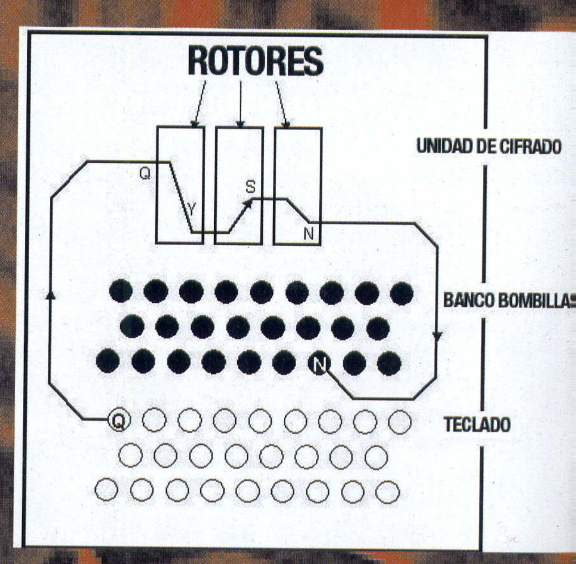


En la dirección http://www.codesandciphers. org.uk/anoraks/index.htm se encuentra toda la información útil, las simulaciones de la máquina Enigma auténtica y los instrumentos informáticos del oficio para llegar a violar el código de la máquina. A quien le gusten los retos encontrará un paraíso. Y del siglo pasado, con aire retro.



Pocos saben que Enigma nació en 1923 con fines comerciales, destinada a las finanzas confidenciales, obra de un tal Arthur Scherbius. Su funcionamiento tenía que ser muy simple: un operador pulsava una letra en claro y se encendía una bombilla que indicaba la letra en cifrado. Bastaba tomar nota de las letras cifradas para construir el mensaje. En realidad esta primera versión no llegó a construirse.

Cada letra pulsada activaba un circuito específico, que pasava tensión a uno de los 26 contactos presentes en la unidad de cifrado. Desde allí la señal atravesaba tres rotores, cada uno de los cuales cambiaba la letra que llegaba en otra. Tras cada letra el primer rotor avanzaba una posición; cada 26 letras lo hacía el segundo, y cada 676 letras, el tercero. Esto hacía que en un mensaje de longitud normal era imposible tener dos letras cifradas igual.



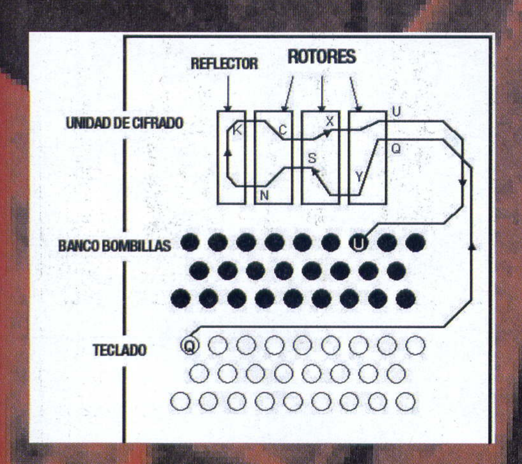
El primer proyecto de Enigma. La flecha indica el recorrido de la información y del cifrado de la letra. La mecánica de cifrado cambia tras cada tecla pulsada.



simple y eficaz

Enigma tenía que ser de fácil uso, pero este proyecto hacía difícil la ingeniería de la decodificación. Así se invirtió la secuencia de los rotores y se añadió un rotor de reflexión, que volvía a mandar la señal dentro de los rotores. Enigma se construyó con este proyecto. Una solución simple y elegante, pero que contenía un grave defecto. El rotor de reflexión implicaba que ninguna letra podía codificarse por sí sola.

De lo comercial a lo militar



↗ *El proyecto de Enigma usado por el ejército alemán, con la adición de un reflector al final de la secuencia de los rotores. Luego se añadieron otros dos rotores.*

El ejército alemán pronto se interesó por Enigma, que se retiró del comercio y se complicó con un mecanismo adjunto llamado Stecker, que intercambiaba copias de letras entre sí. Los alemanes siguieron trabajando en ello y añadieron otros dos rotores facultativos, que permitían elegir tres rotores de los cinco disponibles, y luego se llegó – en 1942 – a la introducción de un cuarto rotor efectivo, que reforzaba mucho el cifrado. Sin embargo, se mantenía el fallo que contribuiría al descifrado y a la derrota bélica.

Falsa seguridad

Los alemanes pensaban que Enigma era inviolable. Se equivocaban. Los primeros en enfrentarse con su cifrado fueron los polacos, cuando por error Alemania envió a un diplomático en Varsovia un despacho de Enigma por correo ordinario. Las insistentes peticiones alemanas para recuperar el paquete sospechoso hicieron sospechar a los aduaneros polacos, que durante un fin de semana examinaron el mensaje antes de envolverlo de nuevo y devolverlo al remitente.

La seguridad de Enigma no estaba en la construcción de la máquina, sino en el enorme número de estados diversos en los que podía encontrarse, de la diversa disposición de los rotores en su posición inicial hasta las conexiones del Stecker. Pero había puntos débiles. Además del fallo ya descrito, por ejemplo, se pedía a los operadores de la máquina que empezaran cada mensaje transmitiendo dos veces seguidas las tres letras correspondientes a la posición inicial de los rotores. Para los criptoanalistas fue un verdadero regalo.

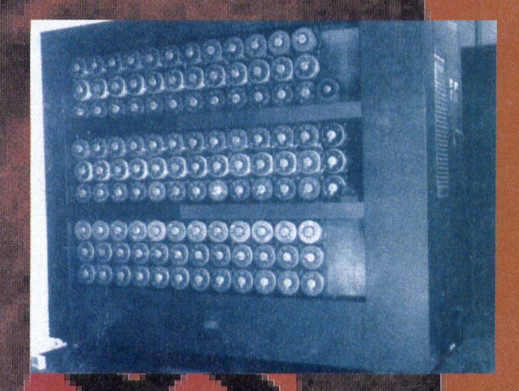
A la caza de pares

Un par es una situación en la que dos letras conocidas (por medio de la repetición inicial) se cifraban en la misma letra. Los polacos construyeron una máquina, llamada bomba, con circuitería parecida a la de Enigma, que podía tener en cuenta los pares y hacerlos corresponder con todas las posibles posiciones de los rotores hasta que se encontraba la correcta. Se requería una bomba por cada ordenación de los rotores; así, con tres rotores, se necesitaban seis bombas. Enigma se hizo segura en diciembre de 1938, cuando se añadieron otros dos rotores. Los polacos no podían construir sesenta bombas. Llegaba el momento de los ingleses.

El Turing club

En enero de 1939, a consecuencia de un encuentro de espionaje polaco, francés e inglés, se dispuso al ataque de Enigma la British Government Code & Cypher School, con la ayuda de uno de los más grandes matemáticos de todos los tiempos, Alan Turing. Los ingleses construyeron las sesenta bombas necesarias y progresaron, con una nueva versión llamada Bombe.

La Bombe era más rápida e inteligente, capaz de aplicar criterios de probabilidad a los mensajes cifrados. De hecho, en contra de las especificaciones del gobierno alemán, los mensajes de Enigma empezaban con las mismas palabras. La capacidad de la Bombe y las debilidades de Enigma bastaron para violar el código y contribuir a la derrota de Hitler. Pero no era trivial; al final de la guerra, cerca de Bletchey Park, sede del descifrado inglés, ¡trabajaban más de 10 000 personas por turnos las 24 horas del día!



↗ *La Bombe, máquina usada por los ingleses para descifrar Enigma, en la que contribuyeron los servicios secretos polacos y el célebre matemático Alan Turing. Pesaba una tonelada.*



Escuchar a la POLICIA

A la caza de frecuencias prohibidas, sin ninguna experiencia y equipados con nuestras propias armas: PC y conexión



Lunes, a las 12,57: una patrulla acaba de girar la esquina ante el escaparate de McDonald's. Un chico de color se gira con los ojos desorbitados y echa a correr. El agente acelera, y lo adelanta. Mientras el conductor llama a la central, su compañero está ya procediendo a detener al chico. Una rápida pesquisa y luego el envío del informe a la central. "Ok, dame el número" "uno-tres-siete-cinco..." "Ok, recibido." y tal, al estilo americano, ya se entiende la idea.

Dos minutos más tarde la vida sigue. La misma patrulla, la misma zona. De nuevo control, y un nuevo intercambio de números. Ahora llama ella, la voz femenina de la central siempre tranquila ante todo, profesional, casi reconfortante.

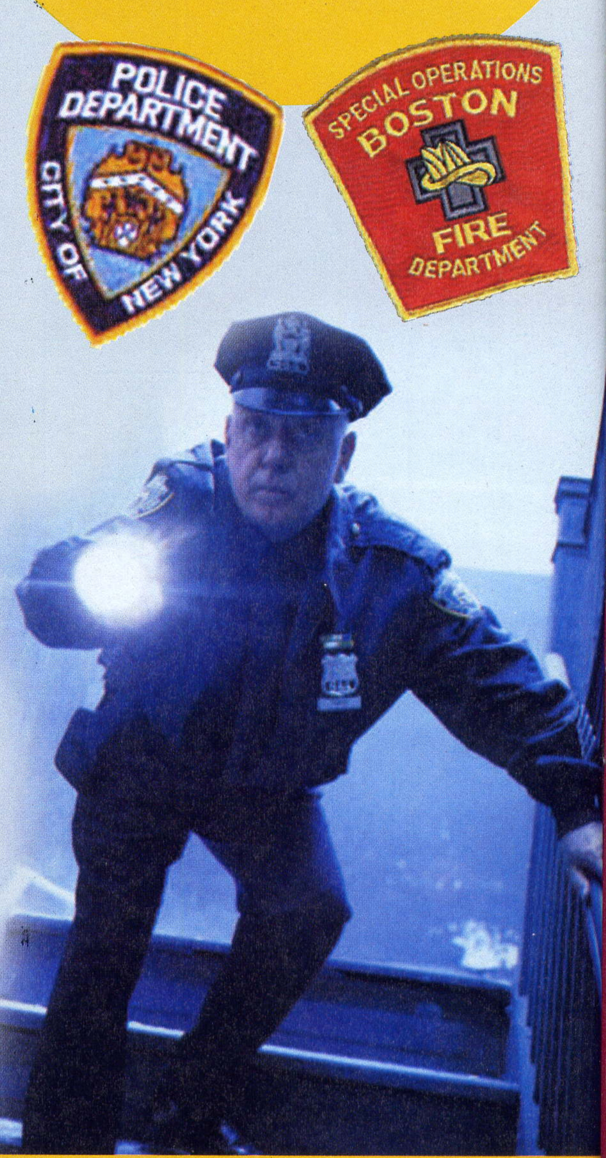
¡Estás escuchando la policía de Nueva York, colega! Y en directo, en la dirección http://www.silive. com/policescanner/

Quién está detrás

Los americanos, ¡naturalmente! Es una batida, pero hasta cierto punto. No sabemos en qué otro país del mundo existe libertad suficiente para consentir cosas de este tipo: en España no, por ejemplo. Tenemos prohibida la radioescucha hasta de las frecuencias que, publicadas en el boletín oficial y por ello de dominio público, permitirían interceptar la radio de los servicios públicos, policía incluida.

Sin embargo, la venta de radio escáneres es libre entre nosotros. En suma, no es recomendable escanear en las cercanías de un aeropuerto militar, pero si estás por ejemplo en tu propia casa, difícilmente nadie llegará a controlarte. Por el simple hecho que la radioescucha no produce perturbaciones de ningún tipo y, se supone, nadie pondrá en Internet lo que ha conseguido captar. Sí pero, ¿quién lo hace? La policia de Nueva York, por su parte, está en la red, 24 horas al día, todos los días de la semana. Al igual que los bomberos y prácticamente todas las estaciones de tierra de los principales aeropuertos de Estados Unidos. Pero la cosa no acaba aquí. Están en línea los aeropuertos militares, de los que se pueden oir las conversaciones, informes técnicos, entre la torre de control y los pilotos que están aterrizando o despegando.

Pero es cierto que lo que se oye, sin quitarle la emoción del curioseo, es todo previsible. Queremos creer que las verdaderas transmisiones críticas viajen cifradas a través de la tecnología adecuada, como ocurre con la policía local.





REALIZAR UN PROGRAMA QUE OCULTA TEXTOS EN UNA IMAGEN

OCULTANDO UN ARCHIVO



En el pasado, ocultar un mensaje en otro tenía un vago aire de misterio y magia, pero aún hoy no todos tienen claro cómo puede funcionar este proceso. ¡Veámoslo juntos!

El término Esteganografía deriva del griego y significa "escritura oculta".

La esteganografía tiene varias formas; en informática se usa en general la esteganografía sustitutiva, que es aquella en la que se sustituyen datos para ocultar otros. Se trata de técnicas útiles para **ocultar textos u otros dentro de documentos no sospechosos como, por ejemplo, imágenes, audio o clips**. Ante los cada vez más frecuentes discursos sobre la inseguridad en Internet, la esteganografía permite transmitir documentos reservados o personales manteniéndolos así y no dejándolos al alcance de cualquiera.
Pasando a la práctica (para la teoría de la esteganografía, recomendamos interrogar los motores de búsqueda de Internet) examinaremos en este artículo los principios básicos para realizar un programa de esteganografía.

» Ocultar los datos

Cualquier documento digital en cualquier plataforma, es visto por el PC como una secuencia de bytes. Ya sea un texto o un programa, no es más que una secuencia de caracteres. Visto esto, se puede empezar diciendo que si se quiere meter un documento dentro de otro hay que hallar un compromiso: **o se añade algo o se modifica algo**. El sistema más eficiente y menos evidente consiste en codificar un documento dentro de una imagen. Ésta es también una secuencia de bytes. Si examinamos una imágen en color, generalmente de 24 bits por píxel, tenemos 3 bytes por cada píxel. Cada byte representa el nivel del color primario al que se refiere.
Por ello, un byte indicará el nivel del componente rojo, otro el verde y otro el azul, que son los colores primarios. Al decir que cada píxel tiene 3 bytes, que indican cada uno el componente cromático, se entiende que una variación de los valores de cada byte corresponde a una variación de la imagen. Si es mínima, es imperceptible al ojo humano.
Por ello, se modificará sólo el último bit de cada byte de la imagen para insertar un bit de texto a ocultar.

0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240	255
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Cada byte (en la columna) indica el nivel del color primario al que se refiere. Arriba, los bytes que indican la intensidad del color. Abajo se observa que al variar el último bit en una unidad, corresponde a variaciones de tono imperceptibles. Así es posible descomponer un carácter de texto en los bits de la codificación ASCII y así modificar el último bit de los bytes relativos a los diversos píxels de la imagen para insertarlo.

» Un ejemplo práctico

La imagen se compone de varios bytes, los primeros 8 que analizamos tienen (por ejemplo) los valores siguientes:

[145] [211] [85] [99] [77] [177] [248] [218]

La primera letra del texto a ocultar es la "C" con un valor Ascii 67 que en binario es 0100000011. Descomponiendo en bits el byte de la imagen tenemos como valor del último bit de cada uno lo siguientes valores:

[1] [1] [1] [1] [1] [1] [0] [0]

El programa a realizar deberá pues variar el último bit de los bytes de la imagen, para insertar los bits que, una vez reunidos en grupos de a ocho, darán el byte correspondiente al carácter del texto a ocultar.
Los bytes de la imagen final pueden tener pues valores distintos de los originales; exactamente:

[144] [211] [84] [98] [77] [177] [249] [219]

Al final del proceso tenemos la imagen en la que si el valor del byte en cuestión es un número par, representa –en la fase de reconstrucción del texto– un bit con valor "0", y si no "1".
En base a esta descripción, vemos ahora qué debe hacer el programa para insertar o quitar el texto de una imagen. Hemos elegido no indicar el listado en un lenguaje específico sino en un metalenguaje comprensible a todos para que cada uno realice su programa en el lenguaje que conozca mejor. Los comentarios se insertan entre ## y ##.

El programa de codificación

```
Definir la variable "Texto"
Definir la variable "Imagen"
Definir la variable "NuevaImagen"
Definir la variable "Header" ##Contendrá la parte
de Header de la imagen original##
Leer el contenido del archivo de texto y ponerlo
en la variable "Texto";
Leer el contenido del archivo de imagen, saltar
la parte de Header, poner la parte de datos en la
variable "Imagen"
```

En esta fase, hay que conocer la estructura del formato de imagen usado. Para simplificarse la vida, se puede trabajar con formatos simples como por ejemplo el formato "RAW" de Photoshop, que no tiene Header.

```
Si la longitud del archivo de texto es mayor que
(longitud del archivo de imagen / 8) avisar que
el archivo de imagen es demasiado pequeño y salir
del programa.
Poner "1" en la variable "ContadorTexto"
Poner "1" en la variable "ContadorImagen"
Repetir por el número de caracteres de la varia-
ble "Texto"
  Poner el valor numérico del carácter Nº
("ContadorTexto") de la variable "Texto" en la
variable "BitCar"
  convertir el valor de "BitCar" a binario
  poner "1" en la variable "ContaBit"
Repetir 8 veces
  si el valor del carácter Nº ("ContaBit") de la
variable "BitCar" es igual a "0"
      poner el valor del carácter Nº
"ContadorImagen" en la variable "ByteImagen"
      poner (truncar ("ByteImagen"/2)*2) en la
variable "ByteImagen"
      convertir la variable "ByteImagen" en el
carácter correspondiente a su valor numérico
```

Será necesaria una función externa

```
  en caso contrario
      poner el valor del carácter Nº
"ContadorImagen" en la variable "ByteImagen"
      poner (trunca ("ByteImagen"/2)*2)+1 en la
variable "ByteImagen"
```

Aquí en realidad se debería verificar si el valor resultante es superior a 255, en este caso tendremos un error porque no podemos tener un carácter con valor superior a 255.

```
      convertir la variable "ByteImagen" en el
carácter correspondiente a su valor numérico
```

Será necesaria una función externa

```
    fin "si"

    Agregar 1 a la variable "ContadorImagen"
    ##a continuación uso del sucesivo carácter
mediante este contador##
    Agregar 1 a la variable "ContaBit"
    ##a continuación uso del sucesivo carácter
mediante este contador##
  Fin repetir ##Era: Repetir 8 veces##
Fin repetir ##Era: Repetir por el número de
caracteres de la variable "Texto"##
```

En este punto, la variable "Header" contiene aún la parte de Header de la imagen original; la variable "NuevaImagen" contiene parte de los datos ya codificados para contener el texto; la variable "Imagen" contiene los datos de la imagen original. Ahora se procede a escribir el archivo de la nueva imagen con el texto codificado en su interior.

```
Abrir el archivo (nombre de archivo) en escritura
Escribir en el archivo (nombre de archivo) la
variable "Header"
Escribir en el archivo (nombre de archivo) la
variable "NuevaImagen"
Escribir en el archivo (nombre de archivo) la
variable "imagen" a partir de (caracteres (longi-
tud de la variable "NuevaImagen") + 1)
Cerrar el archivo (nombre de archivo)
```

La composición de las imágenes

Los colores de la luz son rojo, verde y azul; sumados en igual medida se obtiene luz blanca. Este método, llamado síntesis aditiva, se usa para generar colores en todos los dispositivos que emiten luz como los monitores y la TV. Si se observa con una lupa una televisión, se verán separadamente las partes roja, verde y azul que oportunamente combinadas generan las imágenes.

>> Cuestiones generales

Si has tenido la paciencia de leer toda la sección de programación, **estarás preparado para realizar tu propio programa de Esteganografía con el lenguaje que prefieras**.
Como se sugiere en el código, aparecen funciones externas para varias tareas, como la verificación de la exactitud del nombre del archivo según el estándar de la plataforma adoptada, la conversión de un número decimal a binario y viceversa.
El único problema que podemos encontrar está en la codificación de los diversos formatos de archivo que pueden tener un Header que dejaremos inalterado si queremos poder visualizar la imagen.
Entre los formatos de archivo a utilizar, se desaconsejan los formatos que usan compresión (por ejemplo TIFF comprimido en LZW, JPG) porque **el archivo se tendría que interpretar antes de usarlo, y luego producen archivos muy pequeños**, que permiten ocultar me-



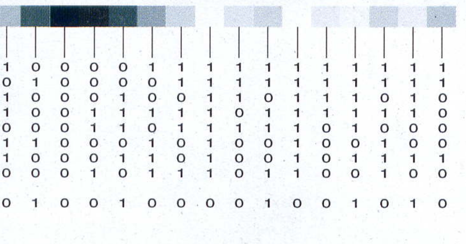
El programa de decodificación

```
Definir la variable "Texto"
Definir la variable "Imagen"
Leer el contenido del archivo de imagen, tras
parte de Header, poner la parte de datos en la
variable "Imagen"
Poner "1" en la variable "ContadorImagen"
##controla qué byte de imagen está examinando##
Repetir para el número de caracteres de la varia-
ble "Imagen"
  Poner 1 en la variable "ContaTexto" ## Cuando
esta variable es igual a 8 significa que se ha
leído un carácter del texto ##
  Poner "" en la variable "CaracterLeido" ##
Inicializa la variabile con el carácter leído ##
  Repetir hasta ("ContaTexto" = 8)
    poner el valor numérico del carácter n°
"ContadorImagen" de la variable "Imagen" en la
variable "NumCar"
    Si (trunca("NumCar"/2))*2 igual a "NumCar" ##
significa que el último bit era "0" ##
       poner "0" tras la variable "CaracterLeido"
    sino
       poner "1" tras la variable "CaracterLeido"
    fin Si
    Agregar "1" a la variable "ContadorImagen"
    Agregar "1" a la variable "ContaTexto"
  Fin repetir ## Repetir hasta (ContaTexto = 8) ##
  Convertir "CaracterLeido" de binario al carácter
correspondiente ## será necesaria una función
externa ##
  Poner "CaracterLeido" tras la variable "Texto"
## la variable "CaracterLeido" contiene un carác-
ter ascii, se escribe al final de la variable
"Texto" que contiene el texto leído ##
Fin repetir ##Era: Repetir por el número de carac-
teres de la variable "Imagen"##
Abrir el archivo (nombre del archivo de texto) en
escritura
## El nombre del archivo podría ser estándar, el
nombre del original más un texto para identificar-
lo o un nombre definido por el usuario. ##
  Escribir en el archivo (nombre del archivo de
texto) la variable "Texto"
Cerrar el archivo (nombre del archivo)
```

nos datos. Conviene usar formatos como el TIFF sin comprimir y el BMP los cuales (tras la sección de header) escriben los datos byte por byte. Para aquellos que no están familiarizados con los formatos gráficos, el formato recomendado es el formato RAW (disponible en diversos programas, como por ejemplo Photoshop también en la versión económica Photoshop Elements) dado que éste **escribe en el archivo sólo los datos de la imagen**. Usando este formato, hay que recordar sin embargo las dimensiones en píxeles de la imagen, dado que no se escriben en el archivo.

>> Conclusiones

Un programa de esteganografía es un óptimo instrumento para mantener oculto lo más privado, desde las cartas de la novia hasta los documentos financieros más reservados. Sin embargo, es necesario recordar que los datos escritos, una vez extraídos, son legibles por cualquiera con otro programa de esteganografía. Si se teme tener cerca algún curioso, puede ser conveniente cifrar los textos usando un programa tipo PGP antes de insertarlo en la image. De este modo, incluso extrayendo los datos, habrá que esforzarse en intentar leerlos y se tendrá una mayor garantía –prácticamente total– de reserva. Si se quiere, se puede insertar en la imagen y así ocultar, no sólo un texto sino también cualquier archivo no TXT.



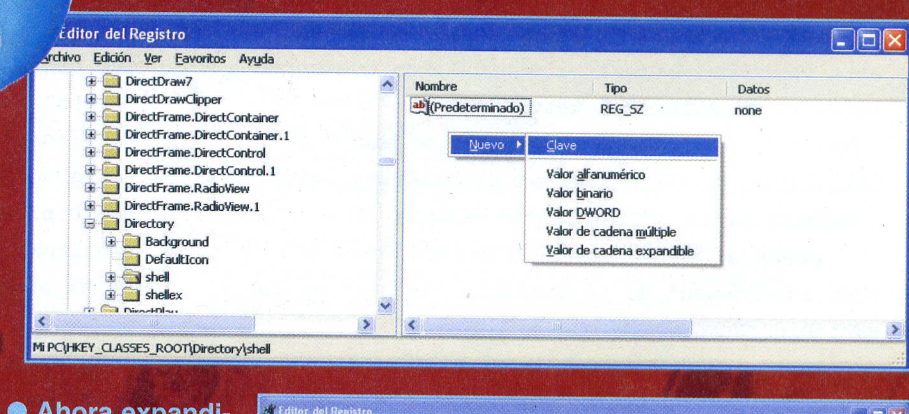
1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1	1	0	1	1	1	0	1	0
1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0
0	0	0	1	1	0	1	1	1	1	1	0	1	0	0	0
1	1	0	0	0	1	0	1	0	0	1	0	0	1	0	0
1	0	0	0	1	1	0	1	0	0	1	0	1	1	1	1
0	0	0	1	0	1	1	1	0	1	1	0	0	1	0	0
0	1	0	0	1	0	0	0	0	1	0	0	1	0	1	0

1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1	1	0	1	1	1	0	1	0
1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0
0	0	0	1	1	0	1	1	1	1	1	0	1	0	0	0
1	1	0	0	0	1	0	1	0	0	1	0	0	1	0	0
1	0	0	0	1	1	0	1	0	0	1	0	1	1	1	1
0	1	0	0	1	0	0	0	0	1	0	0	1	0	1	0
0	1	0	0	1	0	0	0	0	1	0	0	1	0	1	0

Hemos sometido a examen 16 píxeles de una imagen y se muestra el valor de los primeros 16 píxeles. Para simplificar, hemos tomado una imagen en escala de grises. En la parte superior los datos contenidos en la imagen original donde, mediante modificación, se han insertado las letras "HJ" que tienen respectivamente los valores "0 1 0 0 1 0 0 0" y "0 1 0 0 1 0 1 0". El último byte de cada píxel se modifica si es preciso. A pesar de los cambios, el aspecto general de la imagen queda sin cambios.

CustoM

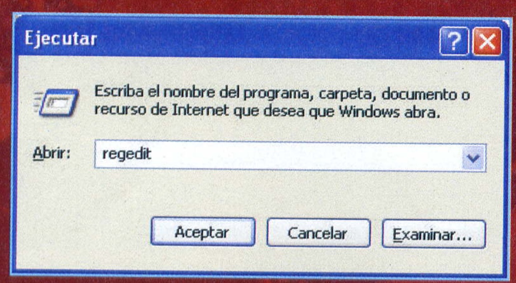
Pulso el botón secundario y hago que Windows haga lo que yo quiero.



● Ahora expandimos la clase del registro HKEY_CLASSES_ROOT. Seleccionamos shell, bajo Directory, y pulsamos en el panel de la derecha. Seleccionamos Nuevo -> Clave.

Se puede configurar el botón secundario del mouse de modo que se ejecuten los comandos que queramos con Windows. Por ejemplo, para activar comandos de Perl. Pero las posibilidades son infinitas, si sabemos qué escribir en el registro y procuramos no equivocarnos.

● Ante todo hay que abrir el editor del registro de Windows, seleccionando Ejecutar del menú Inicio y escribiendo regedit.



● Escribimos el nombre del script o del comando que queremos ejecutar. Es mejor no usar espacios y limitarse a letras y números. Este nombre no se verá durante el trabajo normal y por ello no es necesario que sea un nombre significativo.

● Ahora pulsamos el botón primario sobre el nombre que hemos escrito. En la ventana principal aparecerá un valor (Predeterminado) que pulsamos con el botón secundario, para cambiarlo con Modificar.

● Escribimos en el campo Valor el nombre con que se verá el script o el comando y finalmente pulsamos Aceptar.

● Ahora pulsamos el botón secundario del mouse sobre el nombre no visible, el primero que hemos escrito, y seleccionamos Nuevo -> Clave, y luego escribimos command.

● Pulsamos la carpeta command. Aparecera en la ventana principal otro valor valore (Predeterminado) que pulsamos con el botón secundario para cambiarlo con Modificar.

● Ésta es la parte más importante del proceso: en el campo Información del valor tenemos que escribir el comando exacto que queremos ejecutar con el clic secundario del mouse. Por ejemplo, en el caso de un script perl, podría ser `perl.exe c:\mis documentos\`



RighT ClicK!

scripts\perl\scp-pl. Depende de ti. En cualquier caso, al terminar, tienes que pulsar el botón Aceptar.
Hemos terminado la mayor parte del trabajo. Ahora, cuando Explorer muestra una carpeta, podemos hacer clic con el botón secundario del mouse sobre dicha carpeta y verla en el menú contextual también con el comando que habremos insertado.
Podemos cerrar el editor del registro, ahora. Es bastante sencillo, ¿no crees?

hacerlo con un archivo

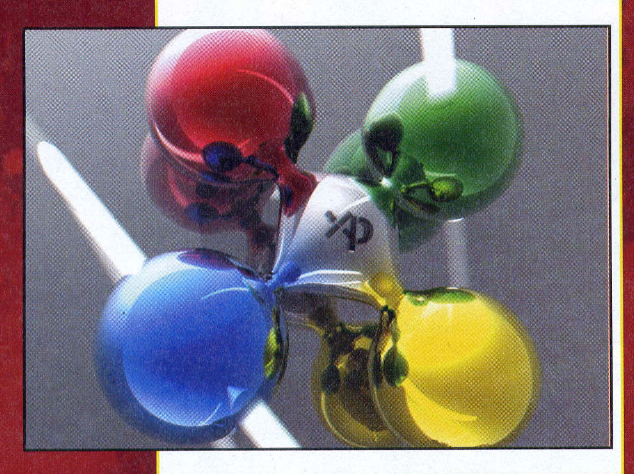
Si preferimos no tocar el registro, podemos hacerlo así: copiamos con cuidado el código que presentamos abajo y lo guardamos en el equipo con Windows con la extensión .reg. Luego hacemos un doble clic sobre el archivo y el registro se actualizará automáticamente, sin que sea necesario que lo abras y manipules manualmente. Naturalmente, si al copiar el texto cometes un solo error, por pequeño que parezca, corres el riesgo de estropearlo todo, por lo que... ¡pon toda tu atención! El ejemplo sigue siendo el de antes, con un script Perl.

SON NUESTROS REGISTROS

Trapichear en el Registro de Windows es PELIGROSO. Si estás distraido, pensando en otra cosa, no eres capaz de releer lo que escribes o piensas que los pequeños errores no cuentan, don't try this at home: no pruebes estas cosas en tu equipo hasta que te hayas centrado.

PROBADO (CASI) EN TODOS

Este truco funciona seguro en Windows 2000 y también en Windows XP. Tendría que funcionar asimismo en las otras versiones de Windows, pero aún no hemos tenido ocasión de probarlo.



REGEDIT4

Hay que sustituir lo que sigue en el cuadro amarillo con la información necesaria.

```
<NOMBREINTERNO> = El nombre de servicio, que nadie verá.
;          Usa sólo letras y números, sin espacios.
;
;<NOMBREVIDEO> = El nombre que aparece en el menú desplegable .
;
;<RUTA>   = La ruta hacia el archivo. Duplica las barras invertidas:
;          por ejemplo, c:\\micky\\prog\\perl\\script.pl

[HKEY_CLASSES_ROOT\Directory\shell\<NOMBREINTERNO>]
@="<NOMBREVIDEO>"

[HKEY_CLASSES_ROOT\Directory\shell\<NOMBREINTERNO>\command]
@="perl.exe <ruta>.pl \"%L\""
```

TIPS

¿HAY ALGO QUE NO FUNCIONA?

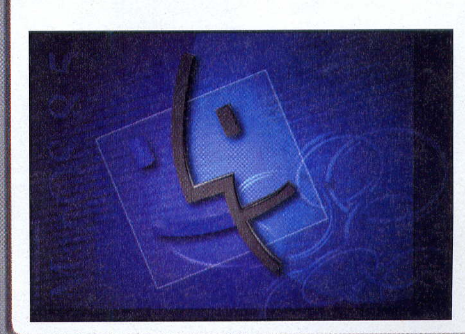
Si en el menú no aparece el comando que has insertado, o bien aparece pero el comando en sí no funciona, es bastante probable que te hayas equivocado al escribir algo. Vuelve al editor del registro y repásalo todo cuidadosamente. Especialmente, la ruta del comando debe ser totalmente correcta.
Para llevar a cabo la prueba definitiva, copia el comando, pégalo en una ventana del prompt de comandos, y comprueba si funciona. Si no funciona tampoco en estas condiciones, significa que algo está mal en el propio comando. Si funciona en el prompt pero no funciona dentro del registro, el comando es correcto pero se ha cometido algún error de escritura.

UNIX Y LA CARPETA SCRIPT

Si usamos sistemas Unix, como Linux o Mac OS X, todo es relativamente más fácil. En Ximian Deskotp de Linux RedHat 8, por poner un ejemplo, existe una carpeta llamada scripts y, si la pulsas con el botón secundario del mouse, aparecerán en el menú contextual todos los scripts disponibles.



En Mac OS X la cosa funciona igual y se recuperan los scripts desde la barra del menú principal.



Windows: no sirve de

Entre quitarle un caramelo a un niño y crackear un PC con Windows, es más complicado conseguir lo del niño. Ni que sea para reirnos un rato, vamos a hablar de los passwords del invento de Redmond.

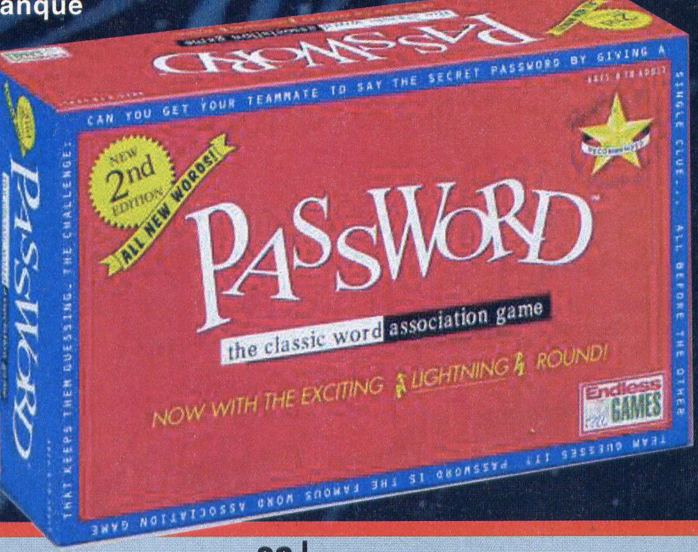
Un cortafuegos bien configurado protege de los accesos externos: cierto. Un antivirus siempre actualizado bloquea ejecutables peligrosos: cierto. Un password largo y lleno de caracteres ASCII mantiene segura cualquier cuenta: ¡falso! En un PC con Windows 95, 98, XP, Me o 2000, hay modos increiblemente simples para superar la pantalla que pide el password para el nombre de usuario.

» Empieza donde yo quiero

Al arrancar un PC, la BIOS busca un disquete o un CD de arranque (depende de la configuración). Cualquiera puede entrar pues con un simple disquete de arranque, por ejemplo el floppy de inicio de la instalación de Windows 9x u otro disco con un sistema ejecutable, insertándolo en la unidad de disquete y arrancando el equipo. Cuando la BIOS deteca un disquete o un CD arrancable, procede a la secuencia hasta el punto en que se pide qué modalidad de acceso queremos usar. Seleccionando el prompt de comandos dispondremos de un shell de DOS con el que podremos hacer de todo.

Para evitar que alguien actúe así, basta con pulsar la tecla ESC (u otra tecla, según el tipo de BIOS) al iniciar el PC y configurar la BIOS para que permita el inicio del PC sólo desde el disco duro, completando el proceso con la asignación de un password para poder entrar en la configuración de la BIOS. Las operaciones a realizar cambian según la placa madre utilizada, pero normalmente hay una opción "Set password" en las opciones "Bios features".

Una vez hecho esto aún no estás seguro, pero al menos habrás reducido el riesgo. Desafortunadamente, hay otros métodos algo más complicados que pueden adoptarse para abrir un boquete en Windows.



» Una tecla y el inicio va OK

Si al arrancar el PC pulsas la tecla F8, te encontrarás ante una pantalla que permite elegir qué hacer: inicio en modo a prueba de fallos, con soporte de red y, lo que nos interesa aquí, línea de comandos en modalidad a prueba de fallos. Selecciónalo y podrás disfrutar el cómodo shell del DOS.

Ahora, piensa que cualquiera podría hacerlo como tú y comprenderás que sin tu password tendrías acceso a tu querido equipo.

Para evitar que suceda, es preciso evitar el archivo C:\msdos.sys. En la entrada [Options] modifica BootKeys=1 con BootKeys=0 (si no está la línea BootKeys=1, créala). Pon atención al hecho que msdos.sys es un archivo normalmente invisible, por lo que será necesario activar la visualización

el password NADA

```
Based on Diku Mud, created by Hans Henrik St{rfeldt, Katja Nyboe, Tom Madsen,
  Michael Seifert, and Sebastian Hammer.  Merc 2.2 by Kahn, Katchet, Furey
           Chaosium by Alathon, title art courtesy of Ingen

 By what name do you wish to be known? Mewtwo
Did I get that right, Mewtwo (Y/N)? y
New character.
Give me a password for Mewtwo:
Please retype password:
```

de todos los archivos por el menú Ver/Opciones/Capeta/Ver.
Pero es que aún existe otro modo para penetrar en tu PC, aunque esta vez es algo más complejo.

>> Y si te pongo la zancadilla...

Si Windows no se inicia con éxito, cuando se inicia de nuevo muestra una pantalla de alarma que permite llegar al mismo menú que aparecía cuando se pulsaba F8 antes. Entonces basta con seleccionar la línea de comandos para obtener el shell de DOS. Esta característica es una medida de seguridad de Windows y no conviene intentar desactivarla.

EL SISTEMA DE PASSWORD DE WINDOWS ES SEGURO COMO TENER EL DINERO BAJO LA ALMOHADA. ¡Y SE APLICA ASIMISMO A TU PROPIO PC!

Para hacer que Windows no se inicie correctamente basta con apagar el equipo durante el proceso de arranque, tras la aparición del logo de Windows. De este modo, se podrá acceder a la pantalla de aviso.
Sin embargo, si quieres intentar bloquear también este intento de ataque, bastará con editar como siempre el archivo C:\msdos.sys, en esta ocasión insertando la línea BootFileSafe=0 siempre dentro de la sección [Options]. Pero esto no es recomendable, porque en caso de cualquier error no podrás reiniciar el PC en modo a prueba de fallos, quedando en una posición la mar de comprometida.

>> Copiar el password

Pero, ¿por qué alguien querría intentar obtener un shell del DOS? El motivo es muy sencillo: si un malintencionado escribiera "format C: " (comando que sirve para borrar todo el contenido del disco duro) habría sonado la hora de que empezaras a lamentarlo profundamente.
O bien podría copiar en A: el archivo de contraseñas. Se trata de archivos con la extensión .pwl que se encuentran en C:\Windows en el caso de Windows 9x.
Por lo tanto, no tendría más que insertar un floppy y escribir:

copy C:\Windows*.pwl A:

El comando copia los archivos con la extensión *.pwl en el floppy.
Una vez en su propio equipo, localizará el archivo *.pwl que corresponde al usuario SERVER. En este caso queda claro que el archivo será SERVER.pwl, porque el nombre tiene 5 caracteres. Si fueran más de 8, se truncaría en la octava letra. Por ejemplo, a un usuario llamado Maximiliano le corresponderá un archivo llamado Maximili.pwl. El archivo está cifrado, pero en Internet los pogramas capaces de descifrarlo se difunden como las (fantásticas) teenager rusas desinhibidas.

REGLA NUMERO UNO: HAZ QUE TE ENCUENTREN

Google

Bastan unas pocas posiciones de más o menos en los motores de búsqueda para decretar el éxito de un sitio. Estos son los trucos para escalar Google sin molestar (casi) a nadie.

Estar en la cima de las búsquedas de Google es importante, y para algunos sitios es cuestión de vida o muerte. Por ejemplo: el sitio de Justin Timberlake debe ir antes que los demás sitios de la gente que se llama Justin o Timberlake o ambas cosas juntas, si no Justin corre el riesgo de vender menos discos y sólo le queda Britney Spears.

Configurar un sitio para que escale en las clasificaciones de Google y los demás motores se ha convertido en una nueva profesión. Se llama SEO, de Search Engine Optimization (optimización para motores de búsqueda), y hay verdaderos profesionales. Hacer un trabajo de SEO como es debido cuesta mucho dinero y ocupa mucho tiempo, pero en este artículo queremos dar algunos consejos simples, al alcance de todos, que pueden mejorar la situación y llevar más arriba un sitio destinado al fondo de todas las búsquedas.

Registrar el dominio adecuado

Tener el nombre adecuado ayuda a que te encuentren. Nombres como quiebra.es, por decir algo, han estado bien por un tiempo, aunque sería mejor laquiebra.es como nombre de dominio. Es decir, si haces un sitio sobre cantantes de rap, dale un nombre genérico, como todorap.

Título correcto, siempre

Las páginas HTML pueden tener un título (tag <title>), que aparece en la barra de título del navegador. Da siempre un título a las páginas del sitio. Que sea un título que hable de lo que hay en la página. ¿Cantantes de rap? "Rap forever: ¡los mejores cantantes están todos aquí!". Si las palabras que pueden buscarse están al principio de la frase, mejor que mejor.

Frames prohibidos

Aunque el programa de creación de páginas lo haga automáticamente, olvídate de los frames. Los motores de búsqueda tienden a evitarlos porque les complican la vida. Más bien, si puedes, usa include. Si no puedes, aprende. O bien prepara páginas más simples, que funcionarán mejor. Conviene construir buenos sitios para los motores de búsqueda. Sí, hay sitios en los primeros sitios con frames, pero su éxito no depende de ellos.

Bajo (con) las metatag

Las metatag son etiquetas de la serie <meta>. Si observas el código fuente de una página profesional verás algo así:

```
<META name="description" content="laquiebra.es: directorio y economía de las empresas en crisis">
<META NAME="keywords" CONTENT="consultoría, directorio, consultoría de quiebra, crédito, débito, deudas">
```

La parte keywords contiene todas las palabras y frases que según los organizadores del sitio buscará la gente en Google relacionadas con las cuestiones de quiebras. Dotar a cada página del sitio con una lista consistente de palabras adecuadas puede ayudar mucho. Las palabras deberán ser coherentes con el alcance del sitio. Escribir "sexo" en el keyword de un sitio sobre rap no tiene sentido, aunque el sexo sea un argumento muy buscado en Internet, porque nadie escribe "sexo" para llegar a sitios sobre rap. Mejor: rap, busta rhymes, eminem, música alternativa, música negra, ritmo... ¿se entiende el concepto?

EN BUSCA DE LA NADA ABSOLUTA

Esta nos la contó un alto directivo de un conocido buscador. ¿Sabes cuál es la palabra más buscada en el buscador? ¿Sexo, música, mp3, film...? Ninguna de ellas. Es " ", nada, cero, cadena vacía, null. La operación más común es pulsar Buscar sin escribir nada en el campo de búsqueda. No está mal, ¿eh?

Los viejos trucos de antes

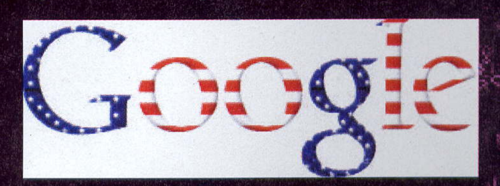
Los sitios porno del pasado tenían la página llena de grandes fondos coloreados sobre los que, con el mismo color y en tamaño microscópico, se escribían miles de términos relacionados con el porno. En la práctica usaban las metatag pero exagerando, para intentar impresionar al motor de búsqueda. Pero ho, este y otros trucos parecidos ya no engañan a los motores. Mejorar ahorrarse el trabajo. Los buscadores pueden ser tierra de oportunidades, pero no de tontos.

Escribir en pirámide inversa

No es un chiste, ni un especial sobre Faraones. La pirámide inversa es un término técnico en uso entre los que escriben como profesión. Significa, para los simples mortales, "primero las cosas importantes". Un ejemplo: he ido al concierto de Eminem en mi viaje a Nueva York y quiero hablar de él en mi blog. Veamos el esquema que solemos utilizar, al estilo de la mejor escuela española:

"Ayer llovía a mares pero me metí en el metro lleno de entusiasmo, porque iba con tiempo más que suficiente y me gusta llegar al teatro pronto. Llegar pronto significa conseguir sitio en la primera fila, desde donde se ve mejor la expresión del cantante..." La gente en Internet lee un poco y lo deja rápido. También los motores de búsqueda. ¡Lo importante va al principio! Probemos:

"¡Gran concierto rap de Eminem en Nueva York ayer noche! Pude ver la expresión de su cara de cerca porque estaba en primera fila. Por suerte tomé el metro temprano. Llovía, pero ¿a quién le importa?". Has visto



que el rap está al principio? El motor de búsqueda no piensa leerlo todo. Mira el principio y luego... ¡adiós!

Esto es sólo el principio. Ante todo: 1) mira dónde está tu sitio ahora; 2) pon en práctica los consejos; 3) espera un par de semanas o tres y observa los progresos. Así sabrás si estás en la senda correcta.

NEWS

GOOGLE INTENTA... QUE NO LE ENGAÑEN

El trabajo de un buen experto de SEO nunca termina, por un motivo: a veces los motores lo cambian todo y hay que empezar de nuevo. Periódicamente, por ejemplo, Google efectúa una revisión de sus criterios de búsqueda y, de la noche al día, ciertos sitios se hunden o surgen de la niebla. Ocurre porque, al revisar los criterios, tal vez cambia la consideración dada a un truco de SEO en favor de otro, o el análisis de contenidos de las páginas varía aunque sea poco. Es suficiente para montar una revolución. Si se hace SEO honestamente no se corre prácticamente riesgo. Quien intenta forzar el mecanismo y hacer trampas, se encontrará patas arriba. En Google son muy listos.

ARAÑAS EN MARCHA POR CUENTA DE G.

En grandes líneas, los motores de búsqueda actualizan sus bases de datos por medio de programas llamados spider (arañas), que viajan continuamente por el Web, leyendo los contenidos de los sitios y pasando los resultados al motor propiamente dicho. Internet es enorme, crece continuamente, y a veces ciertos segmentos de la red se bloquean, por ello las arañas no conseguirán llegar a todas partes simultáneamente. Además, los sitios considerados importantes o que se actualizan más a menudo se visitan primero. De media, un sitio hecho en casa se visita cada dos o tres semanas o como mucho cada tres meses. Por ello, no esperes progresos inmediatos: se requiere paciencia.



Falta una página